

Naše zn. 61441/2023-SŽ-GŘ-O8

Vyřizuje Mgr. Veronika Zajíčková

ZADÁVACÍ DOKUMENTACE

k nadlimitní sektorové veřejné zakázce na dodávky zadávané v otevřeném řízení podle § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), s názvem

„Log management a SIEM“

(dále jen „**zadávací dokumentace**“ a/nebo „**ZD**“)

Identifikační údaje Zadavatele a osoby zastupující Zadavatele

Název: **Správa železnic, státní organizace**

Sídlo: Dlážděná 1003/7, Praha 1 – Nové Město, PSČ 110 00

IČO: 709 94 234

DIČ: CZ 70994234

Zapsaný v obchodním rejstříku vedeném Městským soudem v Praze oddílu A, vložce 48384

Zastoupen: Bc. Jiřím Svobodou, MBA, generálním ředitelem

Profil Zadavatele: <https://zakazky.spravazeleznic.cz/>

1. Druh veřejné zakázky a zadávacího řízení

1.1. Hlavní předmět veřejné zakázky ve smyslu § 15 ZZVZ odpovídá veřejné zakázce na dodávky.

1.2. Zadavatel zadává veřejnou zakázku v souvislosti s výkonem své relevantní činnosti ve smyslu § 153 odst. 1. písm. f) ZZVZ. Jedná se proto o sektorovou veřejnou zakázku.

1.3. Veřejná zakázka je v souladu s § 56 a násl. ZZVZ zadávána jako nadlimitní sektorová veřejná zakázka na dodávky v **otevřeném řízení** ve smyslu § 3 písm. b) ZZVZ.

2. Osoby podílející se na vypracování zadávací dokumentace

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským
soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

2.1. Na zpracování zadávací dokumentace se podíleli:

2.1.1. Zadávací dokumentace, vyjma příloh č. 1, 2, 3, 4, 5, 9, 17, 18, 19, 20 a 21 – CÍSAŘ, ČESKA, SMUTNÝ s.r.o., advokátní kancelář, IČO: 481 18 753, se sídlem Hvězdova 1716/2b, 140 00 Praha 4.

2.1.2. Přílohy č. 1, 2, 3, 5, 9, 17, 19, 20 a 21 této zadávací dokumentace – Corpus Solutions a.s., IČO: 257 64 616, se sídlem Štětкова 1638/18, 140 00 Praha 4.

3. Výsledek předběžné tržní konzultace

3.1. Před zahájením tohoto zadávacího řízení organizoval Zadavatel ve smyslu § 33 ZZVZ předběžnou tržní konzultaci (dále jen „**PTK I**“) s dodavateli, a to písemnou formou (informace o konání PTK I byla uveřejněna na profilu zadavatele – viz https://zakazky.spravazeleznic.cz/contract_display_12111.html). Zadavatel v této souvislosti obeznámil neomezený okruh potenciálních dodavatelů se svým záměrem a potřebami prostřednictvím dokumentu Předběžná tržní konzultace: „Log Management“ (dále jen „**Pozvánka I**“).¹ Pozvánka I rovněž obsahovala přílohu obsahující otázky pro písemnou část PTK I. Dodavatelé, kteří projevíli zájem účastnit se PTK I, měli Zadavateli zasílat své odpovědi na dotazy uvedené v příloze č. 1 Pozvánky I, a to ve stanoveném termínu. Zadavatel následně obdržené odpovědi dodavatelů na dotazy zanalyzoval a získané informace zohlednil v zadávacích podmínkách veřejné zakázky. Tímto způsobem bylo realizováno pouze první kolo PTK I. Druhé kolo PTK I již neproběhlo.

3.2. PTK I se zúčastnili následující dodavatelé:

3.2.1. **ALEF NULA, a.s.**, IČO: 618 58 579, se sídlem Pernerova 691/42, 186 00 Praha 8, Karlín;

3.2.2. **O2 Czech Republic a.s.**, IČO: 601 93 336, se sídlem Praha 4 – Michle, Za Brumlovkou 266/2, 140 22;

3.2.3. **AXENTA a.s.**, IČO: 283 49 822, se sídlem Mlýnská 326/13, Trnitá, 602 00 Brno;

3.2.4. **Caleum a.s.**, IČO: 283 51 363, se sídlem Italská 438/36, Žižkov, 130 00 Praha 3;

3.2.5. **COMGUARD a.s.**, IČO: 043 05 426, se sídlem Sochorova 3209/38, Žabovřesky, 616 00 Brno;

3.2.6. **NEWPS.CZ s.r.o.**, IČO: 256 25 632, se sídlem Vyskočilova 1422/1a, Michle, 140 00 Praha 4;

3.2.7. **Next Generation Security Solutions s.r.o.**, IČO: 062 91 031, se sídlem U Uranie 954/18, Holešovice, 170 00 Praha 7;

3.2.8. **Rexonix security s.r.o.**, IČO: 098 28 052, se sídlem Pod višňovkou 1661/35, Krč, 140 00 Praha 4.

3.2.9. **AMI Praha a.s.**, IČO: 257 15 909, se sídlem Hanusova 826/29, Michle, 140 00 Praha 4.

3.3. Zadavatel prostřednictvím dokumentů, které byly uveřejněny na profilu zadavatele, seznámil dodavatele se svým záměrem realizovat veřejnou zakázku a cílem, jehož má být prostřednictvím veřejné zakázky dosaženo.

3.4. V rámci PTK I Zadavatel ověřoval:

¹ PTK I měla odlišný název, avšak vztahuje se k této veřejné zakázce.

3.4.1. údaje pro řádné nastavení specifikace předmětu plnění a jeho rozsahu a parametrů poptávaných služeb, a

3.4.2. vhodnost spojení aktivity SIEM s realizací řešení Log managementu.

3.5. Na základě informací sdělených v rámci PTK I Zadavatel:

3.5.1. rozhodl o spojení aktivity Log managementu a aktivity SIEM do jedné veřejné zakázky; a

3.5.2. upravil technickou specifikaci předmětu plnění veřejné zakázky.

3.6. Dále před zahájením tohoto zadávacího řízení organizoval Zadavatel ve smyslu § 33 ZZVZ další předběžnou tržní konzultaci (dále jen „**PTK II**“) s dodavateli, a to písemnou formou (informace o konání PTK II byla uveřejněna na profilu zadavatele – viz https://zakazky.spravazeleznic.cz/contract_display_12944.html). Zadavatel v této souvislosti obeznámil neomezený okruh potenciálních dodavatelů se svým záměrem a potřebami prostřednictvím dokumentu Předběžná tržní konzultace: „Log Management a SIEM“ (dále jen „**Pozvánka II**“). Pozvánka II rovněž obsahovala přílohu č. 1 obsahující rámcovou specifikaci předmětu plnění veřejné zakázky a způsob jeho realizace, přílohu č. 2 obsahující otázky pro písemnou část PTK II, přílohu č. 3 obsahující dokument „Platforma SŽ 2.0: Vymezení služeb“, přílohu č. 4 obsahující dokument „Požadavky dodavatele na Platformu SŽ“, a přílohu č. 5 obsahující dokument „Zvláštní obchodní podmínky (ZOP)“. Dodavatelé, kteří projevíli zájem účastnit se PTK II, měli Zadavateli zasílat své odpovědi na dotazy uvedené v příloze č. 2 a 4 Pozvánky II, a to ve stanoveném termínu. Zadavatel následně obdržené odpovědi dodavatelů na dotazy zanalyzoval a získané informace zohlednil v zadávacích podmínkách veřejné zakázky. Tímto způsobem bylo realizováno první kolo PTK II. Druhé kolo PTK II již neproběhlo.

3.7. PTK II se zúčastnili následující dodavatelé:

3.7.1. **ALEF NULA, a.s.**, IČO: 618 58 579, se sídlem Pernerova 691/42, 186 00 Praha 8, Karlín;

3.7.2. **O2 Czech Republic a.s.**, IČO: 601 93 336, se sídlem Praha 4 – Michle, Za Brumlovkou 266/2, 140 22;

3.7.3. **COMGUARD a.s.**, IČO: 043 05 426, se sídlem Sochorova 3209/38, Žabovřesky, 616 00 Brno;

3.7.4. **NEWPS.CZ s.r.o.**, IČO: 256 25 632, se sídlem Vyskočilova 1422/1a, Michle, 140 00 Praha 4;

3.7.5. **Rexonix security s.r.o.**, IČO: 098 28 052, se sídlem Pod višňovkou 1661/35, Krč, 140 00 Praha 4;

3.7.6. **ISECO.CZ s.r.o.**, IČO: 036 41 074, se sídlem Bartůňkova 2349/3a, Chodov, 149 00 Praha 4;

3.7.7. **IXPERTA s.r.o.**, IČO: 275 99 523, se sídlem Lihovarská 1060/12, Libeň, 190 00 Praha 9.

3.8. Zadavatel prostřednictvím dokumentů, které byly uveřejněny na profilu zadavatele, seznámil dodavatele se svým záměrem realizovat veřejnou zakázku a cílem, jehož má být prostřednictvím veřejné zakázky dosaženo.

3.9. V rámci PTK II Zadavatel ověřoval:

3.9.1. údaje pro řádné nastavení specifikace předmětu plnění a jeho rozsahu a parametrů poptávaných služeb,

3.9.2. údaje pro řádné určení předpokládané hodnoty veřejné zakázky,

3.9.3. údaje ohledně předpokládaných požadavků na virtualizační prostředí IT Infrastruktury Zadavatele,

3.9.4. údaje pro správné nastavení harmonogramu plnění, a

3.9.5. údaje umožňující určit nezbytnou úroveň podpory řešení.

3.10. Na základě informací sdělených v rámci PTK Zadavatel:

3.10.1. upravil technickou specifikaci předmětu plnění veřejné zakázky, a

3.10.2. stanovil předpokládanou hodnotu veřejné zakázky.

3.11. Shrnutí výsledku PTK I a PTK II (včetně způsobu jejich promítnutí do zadávací dokumentace veřejné zakázky) tvoří Příloha č. 17 této zadávací dokumentace; z této přílohy je přitom patrné i to, jaké konkrétní informace uvedené v zadávací dokumentaci byly realizací PTK I a PTK II dotčeny, resp. upraveny.

4. Účel veřejné zakázky

4.1. Účelem veřejné zakázky je pomocí zavedení řešení Log management a SIEM zajistit jednotný sběr provozních a bezpečnostních událostí z prostředí Zadavatele, čímž bude zajištěna jejich integrita a další požadavky vyplývající ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZoKB**“), a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), v platném znění (dále jen „**VoKB**“), a rovněž zlepšit celkový stav zabezpečení Zadavatele, zajistit soulad s příslušnými bezpečnostními standardy, jež Zadavatel uplatňuje, zefektivnit vyšetřování incidentů a snížit provozní náklady Zadavatele.

5. Předpokládaná hodnota

5.1. Předpokládaná hodnota veřejné zakázky činí **95.000.000 Kč bez DPH**.

5.2. Zadavatel stanovil, že předpokládaná hodnota veřejné zakázky současně představuje maximální a nepřekročitelnou nabídkovou cenu.

5.3. Podání nabídky s nabídkovou cenou v korunách českých bez DPH za předmět této veřejné zakázky vyšší, než je částka dle článku 5.1 této zadávací dokumentace bude Zadavatelem posouzeno jako nesplnění zadávacích podmínek a bude mít za následek vyloučení účastníka ze zadávacího řízení.

6. Předmět plnění veřejné zakázky a další informace

6.1. Předmětem zadávacího řízení je výběr dodavatele a uzavření smlouvy o dílo – Log management a SIEM.

6.2. Předmětem plnění veřejné zakázky je dodávka, implementace a podpora systému Log management a SIEM, které bude zajišťovat jednotný sběr provozních a bezpečnostních událostí z prostředí Zadavatele, uchovávat je pro potřeby analýzy a archivovat je v souladu s požadavky ZoKB a VoKB. Systém SIEM je bezpečnostní nadstavbou nad systémem Log management, který zajišťuje detekci provozních a bezpečnostních událostí, které je možné odvodit od struktury posloupnosti a významu zaznamenaných logů nebo na základě předem definovaných symptomatických pravidel.

6.3. Bližší specifikace předmětu plnění veřejné zakázky je uvedena v technické specifikaci, která tvoří Příloha č. 1 této zadávací dokumentace (dále jen „**technická specifikace**“), a v závazném vzoru smlouvy, který tvoří Příloha č. 6 této zadávací dokumentace (dále jen „**závazný vzor smlouvy**“).

6.4. Zadavatel provozuje informační systémy kritické informační infrastruktury a předmět plnění veřejné zakázky je určen pro jejich provozování. Zadavatel je proto povinen řídit se ZoKB.

Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“), na základě ZoKB Varování, č. j. 3012/2018NÚKIB-E/110, kde uvedl, že: „*Použití technických nebo programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:*

- *Huawei Technologies Co., Ltd, Šen-čen, Čínská lidová republika*
- *ZTE Corporation, Šen-čen, Čínská lidová republika*“.

Dne 4. ledna 2019 vydal NÚKIB Metodiku k varování ze dne 17. prosince 2018 (dále jen „**metodika**“), kde jsou mj. určeny i postupy pro aktualizaci analýzy rizik. V souladu s vydanou metodikou Zadavatel provedl analýzu rizik související s předmětnou veřejnou zakázkou na dodávky, jak je jeho povinností podle § 5 a § 8 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů. V návaznosti na to Zadavatel identifikoval rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná a současně opatření k jejich zvládnutí, kterým je nepřipustění použití těchto prostředků v rámci plnění veřejné zakázky.

V souladu s § 4 odst. 4 ZoKB Zadavatel zohledňuje požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro Zadavatelem zajišťované služby informačních systémů v kategorii KII (Kritické informační infrastruktury).

Zadavatel tak na základě varování NÚKIB, navazující metodiky a provedené analýzy rizik, ve spojení s § 4 odst. 4 ZoKB, nepřipouští v rámci plnění veřejné zakázky použití technických nebo programových prostředků společností (výrobců), které jsou uvedené v současné době platném varování NÚKIB jako hrozba v oblasti kybernetické bezpečnosti.

Pokud by některý z dodavatelů ve své nabídce nerespektoval zákaz, resp. zadávací podmínku uvedenou v tomto čl. 6.4 zadávací dokumentace, tzn. že by pro plnění veřejné zakázky navrhl použití technických nebo programových prostředků výše uvedených společností (výrobců), Zadavatel bude postupovat podle § 48 odst. 2 písm. a) ZZVZ ve spojení s § 48 odst. 8 ZZVZ a přistoupí k vyloučení takového dodavatele ze zadávacího řízení.

6.5. Klasifikace předmětu veřejné zakázky

- Kód CPV: 48730000-4 Balík programů pro zabezpečení
- Kód CPV: 48732000-8 Balík programů pro zabezpečení dat
- Kód CPV: 48517000-5 Balík programů pro IT
- Kód CPV: 48820000-2 Servery
- Kód CPV: 72317000-0 Ukládání dat
- Kód CPV: 72268000-1 Dodávka programového vybavení
- Kód CPV: 72224100-2 Plánování implementace systémů
- Kód CPV: 72246000-1 Systémové poradenství

- Kód CPV: 72223000-4 Hodnocení požadavků informačních technologií
- Kód CPV: 72253200-5 Systémová podpora
- Kód CPV: 72228000-9 Poradenské služby v oblasti integrace technického vybavení počítačů.

7. Doba plnění a místo plnění veřejné zakázky

7.1. Doba plnění veřejné zakázky

Termín zahájení plnění: Zadavatel předpokládá zahájení realizace plnění veřejné zakázky po ukončení tohoto zadávacího řízení.

Termín ukončení plnění: Doba plnění je 5 let a 4 měsíce od účinnosti smlouvy. Doba plnění však neuplyne dříve než za 5 let od ukončení Etapy 1B podle Příloha č. 5 této zadávací dokumentace.

7.2. Místo plnění veřejné zakázky

Plnění veřejné zakázky bude probíhat především v sídle Zadavatele a v sídlech jednotlivých organizačních složek Zadavatele, nebo na jakýchkoli jiných místech, pokud to bude potřebné či vhodné pro realizaci předmětu plnění veřejné zakázky.

8. Sociálně a environmentálně odpovědné zadávání, inovace

8.1. Zadavatel při vytváření zadávacích podmínek, včetně pravidel pro hodnocení nabídek, a výběru dodavatele, postupoval tak, aby v co nejvyšší možné míře naplnil zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací tak jak jsou definovány v § 28 odst. 1 písm. p) až r) ZZVZ (dále jen „**odpovědné zadávání**“). Vzhledem k tomu, že jednotlivé postupy odpovědného zadávání nebyly v ZZVZ ani v jiném zákoně taxativně vymezeny a současně je odpovědné zadávání stále se velmi dynamicky vyvíjejícím institutem veřejného zadávání, Zadavatel při vytváření podmínek zvažoval použití zejména těch prvků odpovědného zadávání, které byly v době vytváření zadávacích podmínek jednoznačně vymezitelné a vymahatelné, a současně byla u nich vysoká míra jistoty, že Zadavatel jejich aplikací neporuší ostatní zásady uvedené v § 6 ZZVZ a také principy 3E vyplývající ze zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých dalších zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů.

8.2. Zadavatel aplikuje v zadávacím řízení prvky odpovědného zadávání podle čl. 8.3 a 8.4 této zadávací dokumentace. Použití jiných prvků odpovědného zadávání, které byly Zadavateli známy při vytváření této zadávací dokumentace, není vzhledem k povaze a smyslu veřejné zakázky vhodné z těchto důvodů:

8.2.1. V oblasti environmentálního odpovědného zadávání Zadavatel neshledal potřebu použití dílčích aspektů odpovědného zadávání, neboť činnosti, které jsou předmětem této veřejné zakázky, nezatěžují životní prostředí nad rámec běžného života a spotřeba energií, vody, surovin a produkce znečišťujících látek je minimální či žádná.

8.2.2. V oblasti inovací Zadavatel nestanovil dílčí kritéria odpovědného zadávání s ohledem na skutečnost, že v rámci předmětu plnění veřejné zakázky neidentifikoval žádná možná inovativní řešení. Z těchto důvodů jsou inovace u daného předmětu plnění fakticky vyloučeny.

8.2.3. V oblasti sociálně odpovědného zadávání Zadavatel neshledal potřebu použití dalších dílčích aspektů odpovědného zadávání, kromě těch, které jsou uvedeny v čl. 8.3 a 8.4 této zadávací dokumentace, s ohledem na specifičnost těchto služeb, kdy

předmětem služeb je specializované plnění, spočívající zejména v dodávce, implementaci a následné podpoře řešení Log management a SIEM. Vzhledem k těmto důvodům je nutné, aby se na plnění veřejné zakázky podílely osoby s vysokou kvalifikací. Nejedná se tedy o vhodnou příležitost k zaměstnání osob znevýhodněných na trhu práce.

8.3. Rovnocenné platební podmínky v rámci dodavatelského řetězce:

8.3.1. Zadavatel realizuje veřejnou zakázku s ohledem na ochranu malých a středních podniků v případném postavení poddodavatelů, a to formou:

- a. umožnění přímých plateb případným poddodavatelům a
- b. zajištění stejné doby splatnosti faktur pro poddodavatele jako pro vybraného dodavatele.

8.4. Dodržování pracovněprávních předpisů:

8.4.1. Zadavatel stanovuje, že vybraný dodavatel je při plnění veřejné zakázky povinen dodržovat pracovněprávní předpisy, a to zejména, nikoliv však výlučně, předpisy upravující mzdy zaměstnanců, pracovní dobu, dobu odpočinku mezi směnami, placené přesčasy, bezpečnost práce apod. Zadavatel dále vyžaduje zajistit férové pracovní podmínky a odpovídající úroveň bezpečnosti práce pro všechny osoby podílející se na plnění veřejné zakázky. Vybraný dodavatel je povinen zajistit splnění tohoto požadavku Zadavatele i u svých poddodavatelů.

8.4.2. Vybraný dodavatel bude povinen plnění těchto povinností Zadavateli doložit kdykoli do 5 pracovních dnů od výzvy Zadavatele, a to včetně všech potřebných dokladů dle aktuálních právních předpisů, resp. též s příslušnými výstupy ze mzdového a účetního systému vybraného dodavatele.

9. Prohlídka místa plnění:

9.1. Zadavatel neprovádí prohlídku místa plnění ve smyslu ustanovení § 97 ZZVZ, neboť její uskutečnění není pro účely průběhu zadávacího řízení či plnění veřejné zakázky nezbytné.

10. Požadavky Zadavatele na kvalifikaci dodavatelů

10.1. Zadavatel požaduje dle § 73 ZZVZ po účastnících zadávacího řízení předložení dokladů a informací k prokázání splnění kvalifikace.

10.2. Kritéria kvalifikace

Zadavatel požaduje, aby dodavatelé prokázali následující:

- a) základní způsobilost dle § 74 a § 75 ZZVZ
- b) profesní způsobilost dle § 77 ZZVZ
- c) technickou kvalifikaci dle § 79 ZZVZ

10.3. Forma prokazování splnění kvalifikace

10.3.1. Dodavatel prokáže splnění kvalifikace ve všech případech příslušnými doklady, pro dostatečné prokázání postačuje předložení těchto dokladů formou prostých kopií.

- 10.3.2. Za účelem prokázání kvalifikace Zadavatel přednostně vyžaduje doklady evidované v systému, který identifikuje doklady k prokázání splnění kvalifikace (systém e-Certis).
- 10.3.3. Zadavatel v souladu s § 86 odst. 2 ZZVZ vylučuje možnost, aby dodavatelé pro účely podání nabídky požadované doklady o kvalifikaci dle čl. 10 této zadávací dokumentace nahradili písemným čestným prohlášením.
- 10.3.4. Dodavatel může nahradit požadované doklady jednotným evropským osvědčením pro veřejné zakázky ve smyslu § 87 ZZVZ. Vzor jednotného evropského osvědčení je stanoven prováděcím nařízením Komise (EU) 2016/7 ze dne 5. ledna 2016, kterým se zavádí standardní formulář jednotného evropského osvědčení pro veřejné zakázky (dostupný např. na internetové adrese: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0007&from=cs>).
- 10.3.5. Dodavatel není povinen předložit Zadavateli doklady osvědčující skutečnosti obsažené v jednotném evropském osvědčení pro veřejné zakázky, pokud Zadavateli sdělí, ve kterém jiném zadávacím řízení mu je již předložil.
- 10.3.6. Povinnost předložit doklad může dodavatel splnit odkazem na odpovídající informace vedené v informačním systému veřejné správy ve smyslu *zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů*, nebo v obdobném systému vedeném v jiném členském státu, který umožňuje neomezený dálkový přístup. Takový odkaz musí obsahovat internetovou adresu a údaje pro přihlášení a vyhledání požadované informace, jsou-li takové údaje nezbytné. V ČR jde zejména o výpis z obchodního rejstříku, výpis z veřejné části živnostenského rejstříku nebo výpis ze seznamu kvalifikovaných dodavatelů.
- 10.3.7. Dodavatel předkládá doklady prokazující splnění kvalifikace ve formě prosté kopie. Tímto není dotčeno oprávnění Zadavatele dle bodu 24.2.2 této zadávací dokumentace.
- 10.3.8. Doklady prokazující základní způsobilost podle § 74 ZZVZ musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců přede dnem zahájení zadávacího řízení. Tímto není dotčeno oprávnění Zadavatele dle bodu 24.2.2 této zadávací dokumentace.
- 10.3.9. V případech, kdy Zadavatel v rámci prokázání splnění kvalifikace požaduje předložení čestného prohlášení dodavatele, musí takové čestné prohlášení obsahovat Zadavatelem požadované údaje.
- 10.3.10. Pokud ZZVZ nebo Zadavatel požaduje předložení dokladu podle právního řádu České republiky, může dodavatel předložit obdobný doklad podle právního řádu státu, ve kterém se tento doklad vydává. Doklad, který je vyhotoven v jiném jazyce, než který Zadavatel určil pro podání nabídky, se předkládá s překladem do Zadavatelem určeného jazyka. Bude-li mít Zadavatel pochybnosti o správnosti překladu, je oprávněn si vyžádat předložení úředně ověřeného překladu dokladu tlumočnickem zapsaným do seznamu znalců a tlumočnicků podle zákona č. 36/1967 Sb., o znalcích a tlumočnících, ve znění pozdějších předpisů². Povinnost připojit k dokladům překlad se nevztahuje na doklady v českém nebo slovenském jazyce. Doklady o vzdělání, např. vysokoškolské diplomy, lze předkládat rovněž v latinském jazyce. Zadavatel může povinnost předložit překlad prominout i u jiných dokladů. Pokud se podle

² Uvedený právní předpis byl zrušen a nahrazen zákonem č. 254/2019 Sb., o znalcích, znaleckých kancelářích a znaleckých ústavech, ve znění pozdějších předpisů.

příslušného právního řádu požadovaný doklad nevydává, může být nahrazen písemným čestným prohlášením.

10.4. Prokázání kvalifikace prostřednictvím jiných osob dle § 83 ZZVZ

10.4.1. Dodavatel může ekonomickou kvalifikaci, technickou kvalifikaci nebo profesní způsobilosti s výjimkou kritéria podle § 77 odst. 1 ZZVZ požadovanou Zadavatelem prokázat prostřednictvím jiných osob. Dodavatel je v takovém případě povinen Zadavateli předložit:

- a) doklady prokazující splnění profesní způsobilosti podle § 77 odst. 1 ZZVZ jinou osobou,
- b) doklady prokazující splnění chybějící části kvalifikace prostřednictvím jiné osoby,
- c) doklady o splnění základní způsobilosti podle § 74 ZZVZ jinou osobou a
- d) smlouvu nebo jinou osobou podepsané potvrzení o její existenci, jejímž obsahem je závazek jiné osoby k poskytnutí plnění určeného k plnění veřejné zakázky nebo k poskytnutí věcí nebo práv, s nimiž bude dodavatel oprávněn disponovat při plnění veřejné zakázky, a to alespoň v rozsahu, v jakém jiná osoba prokázala kvalifikaci za dodavatele.

10.4.2. Prokazuje-li dodavatel prostřednictvím jiné osoby kvalifikaci a předkládá doklady podle § 79 odst. 2 písm. a), b) nebo d) ZZVZ vztahující se k takové osobě, musí ze smlouvy nebo potvrzení o její existenci podle čl. 10.4.1 písm. d) této zadávací dokumentace vyplývat závazek, že jiná osoba bude vykonávat stavební práce či služby, ke kterým se prokazované kritérium kvalifikace vztahuje.

10.4.3. Má se za to, že požadavek podle čl. 10.4.1, písm. d) této zadávací dokumentace je splněn, pokud z obsahu smlouvy nebo potvrzení o její existenci podle čl. 10.4.1, písm. d) této zadávací dokumentace vyplývá závazek jiné osoby plnit veřejnou zakázku společně a nerozdílně s dodavatelem; to neplatí, pokud smlouva nebo potvrzení o její existenci podle čl. 10.4.1, písm. d) této zadávací dokumentace musí splňovat požadavky podle čl. 10.4.2 této zadávací dokumentace.

10.4.4. Dodavatelé a jiné osoby prokazují (mohou prokázat) kvalifikaci společně.

10.4.5. Dodavatel a jiná osoba, jejímž prostřednictvím dodavatel prokazuje ekonomickou kvalifikaci, nesou společnou a nerozdílnou odpovědnost za plnění veřejné zakázky.

10.4.6. Na kvalifikaci jiné osoby, jejímž prostřednictvím je prokazována kvalifikace, se vztahují pravidla stanovená ZZVZ nebo zadávacími podmínkami pro kvalifikaci dodavatele, za kterého je kvalifikace prokazována.

10.4.7. Zadavatel upozorňuje, že povinnost doložit veškeré doklady uvedené výše v tomto článku zadávací dokumentace platí i v případě, kdy je část kvalifikace prokazována poddodavatelem poddodavatele (pod-poddodavatelem).

10.5. Prokazování kvalifikace v případě společné účasti dodavatelů dle § 82 ZZVZ

10.5.1. V případě společné účasti dodavatelů prokazuje základní způsobilost dle § 74 a § 75 ZZVZ a profesní způsobilost podle § 77 odst. 1 ZZVZ každý dodavatel samostatně.

10.5.2. Nabídka více dodavatelů musí dále splňovat následující předpoklady:

- a) Jeden z dodavatelů bude určen jako vedoucí účastník odpovědný za veřejnou zakázku a toto určení bude potvrzeno předložením zmocnění k zastupování všech ostatních dodavatelů.
- b) Zadavatel vyžaduje, aby odpovědnost za plnění veřejné zakázky nesli všichni dodavatelé podávající společnou nabídku společně a nerozdílně.

10.5.3. V případě, že má být předmět veřejné zakázky plněn společně několika dodavateli, Zadavatel požaduje předložit v nabídce současně s doklady prokazujícími způsobilost a kvalifikaci též smlouvu, ve které je obsažen závazek, že všichni tito dodavatelé budou vůči Zadavateli a třetím osobám z jakýchkoliv právních vztahů vzniklých v souvislosti s veřejnou zakázkou zavázáni společně a nerozdílně, a to po celou dobu plnění veřejné zakázky i po dobu trvání jiných závazků vyplývajících z veřejné zakázky. Smlouva též musí obsahovat úpravu způsobu právního jednání těchto dodavatelů vůči Zadavateli.

10.6. Prokazování kvalifikace získané v zahraničí dle § 81 ZZVZ

10.6.1. V případě, že byla kvalifikace získána v zahraničí, prokazuje se doklady vydanými podle právního řádu země, ve které byla získána, a to v rozsahu požadovaném Zadavatelem.

10.6.2. Výpis z evidence Rejstříku trestů vydává Rejstřík trestů. Potvrzení pro daňové nedoplatky zahraničních dodavatelů v ČR vydává Finanční úřad pro Prahu 1 a potvrzení pro nedoplatky zahraničních dodavatelů v ČR na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti vydává Pražská správa sociálního zabezpečení.

10.7. Změny kvalifikace účastníka zadávacího řízení dle § 88 ZZVZ

10.7.1. Pokud po předložení dokladů nebo prohlášení o kvalifikaci dojde v průběhu zadávacího řízení ke změně kvalifikace účastníka zadávacího řízení, je účastník zadávacího řízení povinen tuto změnu Zadavateli do 5 pracovních dnů oznámit a do 10 pracovních dnů od oznámení této změny předložit nové doklady nebo prohlášení ke kvalifikaci. Zadavatel může tyto lhůty prodloužit nebo prominout jejich zmeškání. Povinnost podle věty první účastníku zadávacího řízení nevzniká, pokud je kvalifikace změněna takovým způsobem, že:

- a) podmínky kvalifikace jsou nadále splněny,
- b) nedošlo k ovlivnění kritérií hodnocení nabídek.

10.7.2. Zadavatel může vyloučit účastníka zadávacího řízení, pokud prokáže, že účastník zadávacího řízení nesplnil povinnost dle čl. 10.7.1 této zadávací dokumentace.

10.8. Výpis ze seznamu kvalifikovaných dodavatelů dle § 228 ZZVZ

10.8.1. Předložení dokladu o zapsání dodavatele do seznamu kvalifikovaných dodavatelů vedeného Ministerstvem pro místní rozvoj dle § 226 až § 232 ZZVZ nahrazuje v souladu s § 228 ZZVZ doklad prokazující profesní způsobilost podle § 77 ZZVZ v tom rozsahu, v jakém údaje ve výpisu ze seznamu kvalifikovaných dodavatelů prokazují splnění kritérií profesní způsobilosti, a základní způsobilost podle § 74 ZZVZ v plném rozsahu. Výpis ze seznamu kvalifikovaných dodavatelů nesmí být k poslednímu dni, ke kterému má být prokázána základní způsobilost nebo profesní způsobilost, starší než tři měsíce.

10.9. Předložení certifikátu dle § 234 ZZVZ

10.9.1. Platným certifikátem vydaným v rámci schváleného systému certifikovaných dodavatelů lze podle § 234 ZZVZ prokázat kvalifikaci v zadávacím řízení. Má se za to, že dodavatel je kvalifikovaný v rozsahu uvedeném na certifikátu.

10.10. Důsledek nesplnění kvalifikace

10.10.1. Dodavatel, který nesplní kvalifikaci v požadovaném rozsahu a ZZVZ a touto zadávací dokumentací požadovaným nebo dovoleným způsobem, bude Zadavatelem z účasti v zadávacím řízení vyloučen.

11. Základní způsobilost dle § 74 a § 75 ZZVZ

11.1. Zadavatel v souladu s ustanovením § 73 ZZVZ požaduje prokázání základní způsobilosti podle § 74 ZZVZ následujícím způsobem:

- a) Způsobilým není dodavatel, který byl v zemi svého sídla v posledních 5 letech před zahájením zadávacího řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 ZZVZ nebo obdobný trestný čin podle právního řádu země sídla dodavatele; k zahlazeným odsouzením se nepřihlíží.

*Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice předložením **výpisu z evidence Rejstříku trestů**.*

- b) Způsobilým není dodavatel, který má v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek.

*Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice a k zemi svého sídla předložením **potvrzení příslušného finančního úřadu a písemného čestného prohlášení ve vztahu ke spotřební dani – vzor čestného prohlášení ve vztahu ke spotřební dani je zpracován jako Příloha č. 16 této zadávací dokumentace**.*

- c) Způsobilým není dodavatel, který má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění.

*Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice a k zemi svého sídla předložením **písemného čestného prohlášení**. Vzor čestného prohlášení je zpracován jako Příloha č. 16 této zadávací dokumentace.*

- d) Způsobilým není dodavatel, který má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti.

*Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice a k zemi svého sídla **předložením potvrzení příslušné okresní správy sociálního zabezpečení**.*

- e) Způsobilým není dodavatel, který je v likvidaci, proti němuž bylo vydáno rozhodnutí o úpadku, vůči němuž byla nařízena nucená správa podle jiného právního předpisu nebo v obdobné situaci podle právního řádu země sídla dodavatele.

*Dodavatel prokazuje splnění podmínek základní způsobilosti v tomto kritériu ve vztahu k České republice předložením **výpisu z obchodního rejstříku, nebo předložením písemného čestného prohlášení v případě, že není v obchodním rejstříku zapsán**.*

11.2. Je-li dodavatelem právnická osoba, musí podmínku uvedenou v odstavci 11.1 písm.

a) splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí podmínku uvedenou shora v odstavci 11.1 písm. a) splňovat:

- a. tato právnická osoba,

- b. každý člen statutárního orgánu této právnické osoby a
- c. osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele.

11.3. Účastní-li se zadávacího řízení pobočka závodu:

- 11.3.1. zahraniční právnické osoby, musí podmínku uvedenou v odstavci 11.1 písm. a) splňovat tato právnická osoba a vedoucí pobočky závodu
- 11.3.2. české právnické osoby, musí podmínku uvedenou v odstavci 11.1 písm. a) splňovat:
 - a. tato právnická osoba,
 - b. každý člen statutárního orgánu této právnické osoby a
 - c. osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele
 - d. vedoucí pobočky závodu.

11.4. Zadavatel nemusí ve smyslu § 75 odst. 2 ZZVZ uplatnit důvod pro vyloučení účastníka zadávacího řízení, i když nesplnil podmínky základní způsobilosti, pokud:

- a. by vyloučení účastníka znemožnilo zadání veřejné zakázky v tomto zadávacím řízení a
- b. naléhavý veřejný zájem, zejména veřejné zdraví nebo ochrana životního prostředí, vyžaduje plnění veřejné zakázky.

11.5. Účastník zadávacího řízení může v souladu s § 76 ZZVZ prokázat, že i přes nesplnění základní způsobilosti podle § 74 ZZVZ nebo naplnění důvodu nezpůsobilosti podle § 48 odst. 5 a 6 ZZVZ obnovil svou způsobilost k účasti v zadávacím řízení, pokud v průběhu zadávacího řízení Zadavateli doloží, že přijal dostatečná nápravná opatření. To neplatí po dobu, na kterou byl účastník zadávacího řízení pravomocně odsouzen k zákazu plnění veřejných zakázek nebo účasti v koncesním řízení.

11.6. Pokud Zadavatel dospěje k závěru, že způsobilost účastníka zadávacího řízení byla obnovena, ze zadávacího řízení jej nevyloučí nebo předchozí vyloučení účastníka zadávacího řízení zruší.

12. Profesní způsobilost dle § 77 ZZVZ

12.1. Zadavatel v souladu s ustanovením § 73 ZZVZ požaduje prokázání profesní způsobilosti dle § 77 ZZVZ následujícím způsobem:

- a) Dodavatel prokazuje splnění profesní způsobilosti ve vztahu k České republice předložením výpisu z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje.

*Dodavatel prokazuje splnění tohoto kritéria profesní způsobilosti předložením **výpisu z obchodního rejstříku či jiné obdobné evidence**.*

12.2. Doklady k prokázání profesní způsobilosti dodavatel nemusí předložit, pokud právní předpisy v zemi jeho sídla obdobnou profesní způsobilost nevyžadují.

13. Technická kvalifikace dle § 79 ZZVZ

13.1. Dodavatel předloží **seznam obsahující významné zakázky**, jehož vzor je upraven jako Příloha č. 7 této zadávací dokumentace, s předmětem plnění a technickými parametry tohoto plnění dle čl. 13.1.1 této zadávací dokumentace, poskytnutých za poslední 3 roky před zahájením zadávacího řízení včetně uvedení:

- ceny,
- doby jejich poskytnutí,
- identifikace objednatele a
- telefonní a e-mailový kontakt na kontaktní osobu každého objednatele pro ověření poskytnutí významné zakázky.

13.1.1. Dodavatel prokáže splnění tohoto kvalifikačního kritéria předložením seznamu významných zakázek poskytnutých dodavatelem za posledních 3 roky před zahájením zadávacího řízení, ze kterého bude vyplývat splnění níže uvedených požadavků. Ze seznamu významných zakázek musí vyplývat, že dodavatel v uvedeném období realizoval

- a. **alespoň 2 významné zakázky**, jejichž předmětem byla dodávka včetně implementace a následná podpora řešení Log management a SIEM, nebo (samotná) implementace a následná podpora řešení Log management a SIEM, pro správce nebo provozovatele informačního systému kritické informační infrastruktury, nebo správce nebo provozovatele významného informačního systému nebo správce nebo provozovatele informačního systému základní služby ve smyslu ZoKB, popř. ekvivalentního zákona členské země Evropské unie, v minimálním finančním objemu alespoň 2.500.000 Kč bez DPH za každou takovou významnou zakázku.

13.1.2. Zadavatel upozorňuje, že doba 3 let před zahájením zadávacího řízení se považuje za splněnou, pokud byla významná zakázka v průběhu této doby úspěšně dokončena. Pokud bude dodavatel prokazovat splnění této podmínky technické kvalifikace nadále probíhající významnou zakázkou, jejímž předmětem je dodávka včetně implementace, nebo (samotná) implementace a následná podpora řešení Log management a SIEM, považuje se doba 3 let před zahájením zadávacího řízení za splněnou, pokud již byla dokončena implementace řešení Log management a SIEM (tzn. řešení bylo uvedeno do provozu) a ze strany dodavatele již dochází pouze k následné podpoře řešení Log management a SIEM (tzn. zakázka jako celek ještě nemusí být zcela dokončena).

13.1.3. Dodavatel nemůže k prokázání splnění tohoto kvalifikačního požadavku použít zakázku, kterou poskytl výlučně prostřednictvím poddodavatele, aniž by se na plnění zakázky podílel.

13.2. Osvědčení o vzdělání a odborné kvalifikaci člena realizačního týmu

13.2.1. Dodavatel dále předloží **seznam členů realizačního týmu**, jehož vzor je upraven jako Příloha č. 8 této zadávací dokumentace, a kteří budou splňovat požadavky dle tohoto článku 13.2 zadávací dokumentace.

13.2.2. Členové realizačního týmu budou odpovědní za činnosti, které bude dodavatel provádět v průběhu realizace veřejné zakázky. **Každá osoba v realizačním týmu může zastávat právě jednu pozici.**

13.2.3. Dodavatel prokáže splnění tohoto kvalifikačního požadavku, pokud doloží, že disponuje **minimálně 6 (od sebe odlišnými) osobami**, jež splňují minimální požadavky uvedené v tabulce níže:

Minimální požadavky na kvalifikaci členů realizačního týmu

Pracovní pozice	Minimální požadavky na člena realizačního týmu
Bezpečnostní architekt (minimálně 1 osoba)	<ul style="list-style-type: none"> • minimálně 5letá praxe v uvedené roli, tj. v roli Bezpečnostní architekt, přičemž obsahem této role byla: <ul style="list-style-type: none"> ◦ odpovědnost za návrh a implementaci bezpečnostních opatření; ◦ integrace nástroje SIEM do systému řízení kybernetické bezpečnosti; ◦ supervize bezpečnostních aspektů při implementaci nástroje Log management a SIEM; • minimálně 1 zkušenost se supervizí bezpečnostních aspektů při implementaci řešení Log management a SIEM; • držitel alespoň jednoho z uvedených certifikátů nebo obdobného certifikátu v oboru kybernetické bezpečnosti (anebo certifikátu vyšší kvality): <ul style="list-style-type: none"> ◦ CISSP ◦ CompTIA Security+ ◦ CISA ◦ CRISC ◦ CIA ◦ Lead Auditor ISMS.
SIEM architekt (minimálně 1 osoba)	<ul style="list-style-type: none"> • minimálně 5letá praxe v uvedené roli, tj. v roli SIEM architekt, přičemž obsahem této role byla: <ul style="list-style-type: none"> ◦ analýza požadavků a návrh systému SIEM; ◦ výběr a implementace SIEM řešení; ◦ konfigurace a správa SIEM infrastruktury; ◦ návrh bezpečnostních pravidel. • minimálně 5 zkušeností s realizací implementace řešení SIEM; • držitel platného certifikátu na úrovni SIEM architekt přímo od výrobce řešení, které dodavatel nabízí (dle dodávaného řešení).
Administrátor SIEM (minimálně 3 osoby)	<ul style="list-style-type: none"> • minimálně 5letá praxe v uvedené roli, tj. v roli Administrátor SIEM, přičemž obsahem této role byla: <ul style="list-style-type: none"> ◦ konfigurace a správa SIEM infrastruktury; ◦ správa připojených zařízení; ◦ monitorování a analýza událostí; ◦ správa uživatelů a přístupových práv; ◦ údržba a aktualizace SIEM systému; ◦ sledování reakce na incidenty.

	<ul style="list-style-type: none"> • minimálně 3 zkušenosti s realizací implementace řešení SIEM od výrobce řešení, které dodavatel nabízí v této veřejné zakázce; • držitel technické certifikace od výrobce řešení Log management a SIEM, které dodavatel nabízí.
Projektový manažer (minimálně 1 osoba)	<ul style="list-style-type: none"> • minimálně 5letá praxe v uvedené roli, tj. v roli Projektový manažer; • držitel platného certifikátu na úrovni PRINCE2 (min. úroveň Foundation) nebo ekvivalentního certifikátu (např. IPMA, PMI).

13.2.4. Dodavatel prokáže splnění tohoto kvalifikačního požadavku předložením následujících dokumentů, z nichž bude vyplývat splnění výše uvedených požadavků:

- Seznam členů realizačního týmu dle čl. 13.2.1 této zadávací dokumentace, a
- Osvědčení/certifikát vyžadovaný dle tabulky výše (pozn. certifikáty je možné předložit v rámci nabídky v anglickém jazyce bez jejich překladu do českého jazyka).

14. Požadavky Zadavatele na způsob zpracování nabídkové ceny:

14.1. Způsob zpracování nabídkové ceny

14.1.1. Zadavatel požaduje zpracovat nabídkovou cenu vyplněním formuláře, který tvoří Příloha č. 9 této zadávací dokumentace (dále jen „**formulář pro vyplnění nabídkové ceny**“).

14.1.2. Za účelem řádného vyplnění formuláře pro vyplnění nabídkové ceny dodavatel do Příloha č. 20 zadávací dokumentace „Log management a SIEM dotazník“ v listu „Licence“ doplní název a počet všech jím nabízených typů licencí, údržby licencí a subskripce licencí v souladu s Přílohou č. 1 této zadávací dokumentace. Celkovou cenu za nabízené licence podle Přílohy č. 20 této zadávací dokumentace včetně ceny za údržbu licencí a technickou podporu výrobce na 60 měsíců nebo subskripce licencí včetně údržby a technické podpory na 60 měsíců nabízené dodavatelem dodavatel doplní do buňky E12 formuláře pro vyplnění nabídkové ceny (Etapa E1) (viz čl. 28 této zadávací dokumentace).

14.1.3. Celková nabídková cena za celou dobu trvání smlouvy, která bude předmětem hodnocení, bude při využití Příloha č. 9 této zadávací dokumentace vypočtena automaticky. Zadavatel však doporučuje dodavatelům, aby výpočet řádně zkontrolovali, neboť na tuto část se vztahuje pravidlo uvedené v čl. 14.1.7 této zadávací dokumentace.

14.1.4. Dodavatel je povinen ve formuláři pro vyplnění nabídkové ceny ocenit všechny položky, přičemž každá z vyplňovaných hodnot musí být vyčíslena jako jedno kladné číslo. Výjimku z uvedeného tvoří pouze Etapa E1 (konkrétně buňka E13 listu „Nabídková cena“ formuláře pro vyplnění nabídkové ceny), kterou může dodavatel ocenit i hodnotou 0, a to v případě, že nebudou z jeho strany dodávány žádné další hardwarové prostředky nad rámec specifikovaných Požadavků na služby Platformy SŽ (viz čl. 18.3 této zadávací dokumentace).

14.1.5. Dodavatel není oprávněn formulář pro vyplnění nabídkové ceny jakkoli měnit.

14.1.6. Nabídková cena bude zahrnovat veškeré náklady nezbytné k řádnému, úplnému a kvalitnímu splnění předmětu této veřejné zakázky, včetně všech rizik a vlivů souvisejících s plněním předmětu této veřejné zakázky. Celková nabídková cena bude rovněž zahrnovat pojištění, garance, daně, cla, poplatky, inflační vlivy a jakékoli další výdaje nutné pro realizaci veřejné zakázky, jako je např. cena za odvoz a uskladnění veškerých zbytkových materiálů, obalů a dalšího odpadu souvisejícího s předmětem plnění veřejné zakázky, likvidaci vyřazených komponent a článků či dopravu.

14.1.7. Za správnost provedení výpočtu celkové nabídkové ceny odpovídá účastník zadávacího řízení.

14.2. Mimořádně nízká nabídková cena

14.2.1. V souladu s § 113 ZZVZ posoudí Zadavatel mimořádně nízkou nabídkovou cenu před odesláním oznámení o výběru dodavatele. Zadavatel požádá účastníka zadávacího řízení o písemné zdůvodnění způsobu stanovení mimořádně nízké nabídkové ceny, bude-li tato v jeho nabídce identifikována. Žádost o zdůvodnění mimořádně nízké nabídkové ceny se považuje za žádost podle § 46 ZZVZ, lze ji doplňovat a vznést opakovaně.

15. Jiné požadavky Zadavatele na plnění veřejné zakázky:

15.1. Využití poddodavatele

15.1.1. Zadavatel požaduje, aby účastník zadávacího řízení v nabídce:

- a) určil části veřejné zakázky, které hodlá plnit prostřednictvím poddodavatelů, a
- b) předložil seznam poddodavatelů, pokud jsou dodavateli známi, a uvedl, kterou část veřejné zakázky bude každý z poddodavatelů plnit. Účastník zadávacího řízení může k tomuto účelu využít vzor seznamu poddodavatelů, který tvoří Příloha č. 15 této zadávací dokumentace.

15.1.2. Vybraný dodavatel je povinen předložit Zadavateli identifikační údaje poddodavatelů, a to nejpozději do 10 pracovních dnů od doručení oznámení o výběru dodavatele. Poddodavatelé, kteří nebyli identifikováni podle věty první a kteří se následně zapojí do plnění veřejné zakázky, musí být identifikováni, a to před zahájením plnění veřejné zakázky.

15.1.3. Seznam poddodavatelů se v případě výběru daného účastníka stane přílohou smlouvy.

16. Varianty nabídky

16.1. Zadavatel nepřipouští varianty nabídky.

17. Závazný vzor smlouvy

17.1. Dodavatel je povinen využít závazný vzor smlouvy, který tvoří Příloha č. 6 této zadávací dokumentace.

17.2. Dodavatel není oprávněn činit změny či doplnění závazného vzoru smlouvy, vyjma údajů, u nichž vyplývá z jejich obsahu povinnost doplnění (označené jako „doplň dodavatel“)

či jiným obdobným způsobem). V případě nabídky podávané společně několika dodavateli je dodavatel oprávněn upravit závazný vzor smlouvy toliko s ohledem na tuto skutečnost; totéž platí, je-li dodavatelem fyzická osoba.

17.3. Dodavatel je povinen závazný vzor smlouvy doplněný dle výše uvedených pokynů učinit součástí nabídky.

18. Způsob hodnocení nabídek

18.1. Kritéria hodnocení

18.1.1. Hodnocení nabídek bude provedeno v souladu s § 114 a násl. ZZVZ podle jejich ekonomické výhodnosti dle níže uvedených dílčích hodnotících kritérií.

18.1.2. Pro hodnocení nabídek se použije bodovací stupnice v rozsahu 0 až 100 bodů. Každé jednotlivé nabídce bude dle dílčího kritéria přidělena bodová hodnota, která bude odrážet úspěšnost předmětné nabídky v rámci dílčího kritéria.

18.1.3. Hodnocení bude provedeno podle dílčích hodnotících kritérií uvedených v následující tabulce:

Kritérium hodnocení	Váha
Nabídková cena	60 %
Požadavky na služby Platformy SŽ	40 %

18.2. Nabídková cena

18.2.1. V rámci dílčího kritéria hodnocení „Nabídková cena“ bude hodnocena „Cena celkem v Kč bez DPH“ stanovená způsobem dle čl. 14 této zadávací dokumentace. Nabídková cena relevantní pro hodnocení nabídky bude v nabídce uvedena ve formuláři pro vyplnění nabídkové ceny na listu „Nabídková cena“ v buňce H19, kde tato se vypočte automaticky.

18.2.2. Jako výhodnější bude v tomto kritériu hodnocena nabídka, která bude obsahovat nižší nabídkovou cenu za plnění v Kč bez DPH.

18.2.3. Nejvýhodnější nabídce, tj. nabídce s nejnižší celkovou nabídkovou cenou ze všech hodnocených nabídek bude přiřazeno 100 bodů. Ostatním nabídkám bude přiřazena bodová hodnota stanovená násobkem čísla 100 a poměru celkové nabídkové ceny předložené v nejvýhodnější nabídce (tj. v nabídce s nejnižší nabídkovou cenou) k celkové nabídkové ceně hodnocené nabídky. Takto získaný počet bodů bude vynásoben váhou dílčího hodnotícího kritéria „Nabídková cena“ a následně matematicky zaokrouhlen na dvě desetinná místa.

18.2.4. Výpočet odpovídá následujícímu vzorci:

$$\frac{\text{Výše nejnižší celkové nabídkové ceny bez DPH}}{\text{Výše hodnocené celkové nabídkové ceny bez DPH}} * 100 * 0,6$$

18.3. Požadavky na služby Platformy SŽ

18.3.1. V rámci hodnotícího kritéria „Požadavky na služby Platformy SŽ“ bude hodnocen počet získaných bodů za dodavatelem definované požadavky nabízeného řešení na virtualizační prostředí IT Infrastruktury Zadavatele (dále jen „**Požadavky na služby Platformy SŽ**“). Požadavky na služby Platformy SŽ dodavatel doplní do listu

„Požadavky“ Příloha č. 19 této zadávací dokumentace podle pokynů stanovených v uvedené příloze, a to v listu „Úvod“ a „Požadavky“.

18.3.2. Požadavky na služby Platformy SŽ budou bodově ohodnoceny dle interní nákladové náročnosti, která se promítá do bodů, které jsou určeny dle Příloha č. 19 této zadávací dokumentace (list „Jednotkové_Body“). Počet bodů znázorňuje míru náročnosti Požadavků na služby Platformy SŽ, přičemž platí, že více bodů znázorňuje vyšší náročnost pro Zadavatele. Celkové bodové ohodnocení dílčího hodnotícího kritéria „Požadavky na služby Platformy SŽ“ se po vyplnění listu „Požadavky“ Příloha č. 19 této zadávací dokumentace zobrazí v buňce C14 listu „Požadavky“ a vznikne tak, že se požadavky dodavatele vyplněné v listu „Požadavky“ automaticky vynásobí počtem bodů, který je uveden v listu „Jednotkové_Body“.

18.3.3. Dodavatel nalezne příklad, jak vyplnit list „Požadavky“ na listu „Příklad“ Příloha č. 19 této zadávací dokumentace. Příklad slouží pouze jako ukázka možného vyplnění a v žádném případě z něj nelze dovozovat závěry pro náročnost Požadavků na služby Platformy SŽ dodavatelů.

18.3.4. Jako výhodnější bude v tomto kritériu hodnocena nabídka, která získá nižší počet bodů na základě výpočtu podle čl. 18.3.2 této zadávací dokumentace a Příloha č. 19 této zadávací dokumentace, neboť čím nižší počet bodů dodavatel získá, tím nižší budou v případě výběru jeho nabídky náklady Zadavatele na vytvoření virtualizačního prostředí IT Infrastruktury potřebné pro realizace dodavatelova řešení Log managementu a SIEM.

18.3.5. Nejvýhodnější nabídce, tj. nabídce s nejnižším počtem bodů ze všech hodnocených nabídek, bude přiřazeno 100 bodů. Ostatním nabídkám bude přiřazena bodová hodnota stanovená násobkem čísla 100 a poměru počtu bodů získaných nejvýhodnější nabídkou (tj. v nabídce s nejnižším počtem bodů za dílčí hodnotící kritérium „Požadavky na služby Platformy SŽ“) k počtu bodů za dílčí hodnotící kritérium „Požadavky na služby Platformy SŽ“ hodnocené nabídky. Takto získaný počet bodů bude vynásoben vahou dílčího hodnotícího kritéria „Požadavky na služby Platformy SŽ“ a následně matematicky zaokrouhlen na dvě desetinná místa.

18.3.6. Výpočet odpovídá následujícímu vzorci:

$$\frac{\text{Nabídka s nejnižším počtem bodů za dílčí hodnotící kritérium "Požadavky na služby Platformy SŽ"}}{\text{Počet bodů za dílčí hodnotící kritérium "Požadavky na služby Platformy SŽ" hodnocené nabídky}} * 100 * 0,4$$

18.4. Celkové hodnocení nabídek

18.4.1. Celkové hodnocení nabídek provede Zadavatel tak, že číselné hodnocení nabídek dle jednotlivých dílčích hodnotících kritérií sečte pro každou nabídku a stanoví pořadí úspěšnosti dodavatelů, přičemž jako nejvhodnější bude vyhodnocena nabídka, která dosáhla nejvyšší celkové bodové hodnoty. Pro vyloučení pochybností Zadavatel uvádí, že jednotlivé hodnoty budou při výpočtech hodnocení zaokrouhlovány vždy na 2 desetinná místa.

18.4.2. V případě, že je více nabídek se shodným číselným ohodnocením v celkovém hodnocení nabídek, rozhodne o pořadí nabídky čas podání těchto nabídek dle článku 22.1 této zadávací dokumentace, přičemž platí, že lépe se umístila ta nabídka, která byla podána dříve.

19. Zadávací dokumentace

19.1. Uveřejnění zadávací dokumentace

19.1.1. V souladu s § 96 odst. 1 a 2 ZZVZ je zadávací dokumentace s výjimkou formulářů dle § 212 ZZVZ zveřejněna na profilu Zadavatele na internetové adrese: <https://zakazky.spravazeleznice.cz/>. Tamtéž budou uveřejňovány i vysvětlení, změny nebo doplnění zadávací dokumentace této veřejné zakázky.

19.2. Neveřejná část zadávací dokumentace

19.2.1. Neveřejná část obsahuje následující dokumenty:

- a. Interní předpis Zadavatele „Provozní politika prvků v působnosti systému řízení bezpečnosti informací“ (Příloha č. 18 této zadávací dokumentace),
- b. Analýza prostředí – architektura prostředí SŽ (Příloha č. 2 této zadávací dokumentace),
- c. Analýza prostředí – popis prostředí sítě UAS (Příloha č. 3 této zadávací dokumentace),
- d. Zdroje logů 2023 – 05 (Příloha č. 21 této zadávací dokumentace),

(dále jen „**neveřejná část zadávací dokumentace**“),

kteřé jsou pro plnění předmětu veřejné zakázky závazné, a které nejsou bez znalosti příslušného hesla dodavatelům zpřístupněny na profilu Zadavatele, toto heslo je možné si pro přípravu nabídky písemně vyžádat u Zadavatele. Zadavatel uveřejnil tyto části zadávací dokumentace na profilu Zadavatele jako složku s názvem „Neveřejná část ZD“ a tuto složku zahesloval. Části zadávací dokumentace ve smyslu tohoto článku budou s ohledem na důvěrné informace v nich obsažené poskytnuty dodavatelům pouze v elektronické podobě, a to výhradně na základě písemné žádosti dodavatele o jejich poskytnutí zaslané společně s podepsaným návrhem Dohody o ochraně důvěrných informací (dále jen „**NDA**“) ze strany dodavatele, a to ve znění obsaženém jako Příloha č. 10 této zadávací dokumentace. Po doručení žádosti včetně podepsaného návrhu NDA umožní Zadavatel dodavateli přístup k částem zadávací dokumentace obsahující důvěrné informace způsobem podrobně popsáním v NDA. Za písemnou žádost dodavatele ve smyslu § 96 odst. 2 ZZVZ je považována žádost dodavatele, jejíž součástí je rovněž podepsaný návrh NDA. Příloha č. 10

19.3. Vysvětlení zadávací dokumentace

19.3.1. Zadavatel může zadávací dokumentaci vysvětlit, pokud takové vysvětlení, případně související dokumenty, uveřejní na profilu Zadavatele, a to nejméně **5 pracovních dnů před uplynutím lhůty pro podání nabídek**.

19.3.2. Pokud žádost o vysvětlení zadávací dokumentace doručí dodavatel ve stanové lhůtě písemnou formou, a to elektronicky, Zadavatel vysvětlení uveřejní prostřednictvím elektronického nástroje E-ZAK, včetně přesného znění žádosti bez identifikace tohoto dodavatele, na profilu Zadavatele. Zadavatel není povinen vysvětlení poskytnout, pokud není žádost o vysvětlení doručena včas, a to alespoň 3 pracovní dny před uplynutím shora uvedené lhůty 5 pracovních dnů. Písemná žádost tedy musí být Zadavateli doručena **nejpozději 8 pracovních dnů před uplynutím lhůty pro podání nabídek**. Pokud Zadavatel na žádost o vysvětlení, která není doručena včas, vysvětlení poskytne, nemusí uvedené lhůty dodržet. Žádost o vysvětlení zadávací dokumentace musí být podána v českém jazyce, na žádost podanou v jiném, než v českém jazyce se hledí jako by nebyla podána včas.

19.3.3. Zadavatel je oprávněn uveřejnit na profilu Zadavatele za podmínek § 99 ZZVZ rovněž změnu nebo doplnění zadávací dokumentace.

19.3.4. Pokud dodavatel požádá o vysvětlení ve vztahu k neveřejné části zadávací dokumentace (viz čl. 19.2 této zadávací dokumentace), Zadavatel vysvětlení rozešle všem dodavatelům, kteří splnili podmínky pro obdržení neveřejné části zadávací dokumentace. V případě, že dodavatel získá přístup k neveřejné části zadávací dokumentace poté, co byl již takový dotaz rozeslán, obdrží spolu s dokumenty obsaženými v neveřejné části zadávací dokumentace i takové vysvětlení zadávací dokumentace.

19.3.5. Zadavatel i v tomto případě není povinen vysvětlení poskytnout, pokud není žádost o vysvětlení doručena včas, a to alespoň 3 pracovní dny před uplynutím shora uvedené lhůty 5 pracovních dnů. Písemná žádost tedy musí být Zadavateli doručena **nejpozději 8 pracovních dnů před uplynutím lhůty pro podání nabídek**. Pokud Zadavatel na žádost o vysvětlení neveřejné části zadávací dokumentace, která není doručena včas, vysvětlení poskytne, nemusí uvedené lhůty dodržet, i tato žádost musí být podána v českém jazyce.

20. Závaznost pokynů Zadavatele

20.1. Informace a údaje uvedené v této zadávací dokumentaci vymezují závazné požadavky Zadavatele na plnění veřejné zakázky. Tyto požadavky je dodavatel povinen plně a bezvýhradně respektovat při zpracování své nabídky. Neakceptování požadavků Zadavatele uvedených v této zadávací dokumentaci může být považováno za nesplnění zadávacích podmínek s následkem vyloučení dodavatele ze zadávacího řízení.

20.2. V případě, že zadávací podmínky obsahují odkazy na specifická označení výrobků a služeb, která platí pro určitého podnikatele (osobu) za příznačná, umožňuje Zadavatel použití i jiných, kvalitativně a technicky obdobných řešení, které naplní Zadavatelem požadovanou funkcionalitu (byť jiným způsobem).

20.3. Pokud jsou v zadávací dokumentaci uvedeny odkazy na normy či technické dokumenty podle § 90 odst. 1 a 2 ZZVZ, je tak učiněno v zájmu přesnosti a srozumitelnosti zadávacích podmínek. Zadavatel u každého takového odkazu v souladu s § 90 odst. 3 ZZVZ připouští nabídnout rovnocenné řešení.

21. Komunikace mezi Zadavatelem a dodavatelem:

21.1. Veškerá komunikace mezi Zadavatelem a dodavatelem musí být v souladu s § 211 ZZVZ vedena pouze písemnou formou, a to elektronicky, s výjimkou případů vymezených v ustanovení § 211 odst. 5 ZZVZ. Doručování písemností a komunikace mezi Zadavatelem a dodavatelem bude ze strany Zadavatele probíhat prostřednictvím elektronického nástroje E-ZAK (na adrese: <https://zakazky.spravazeleznic.cz/>), který splňuje podmínky vyhlášky č. 260/2016 Sb., o stanovení podrobnějších podmínek týkajících se elektronických nástrojů, elektronických úkonů při zadávání veřejných zakázek a certifikátu shody, ve znění pozdějších předpisů. Na komunikaci ze strany dodavatelů učiněnou elektronicky, avšak nikoliv prostřednictvím elektronického nástroje E-ZAK, bude tedy Zadavatel vždy odpovídat prostřednictvím elektronického nástroje.

21.2. Zpracování osobních údajů včetně jejich zvláštních kategorií případně poskytnutých v průběhu zadávacího řízení je Zadavatelem prováděno pouze za účelem zadání veřejné zakázky, přičemž Zadavatel v celém procesu ochrany osobních údajů postupuje v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení

směrnice 95/46/ES, obecně závaznými právními předpisy a vnitřními předpisy zadavatele, které agendu ochrany osobních údajů upravují.

21.3. Za řádné a včasné seznamování se s písemnostmi zasílanými Zadavatelem prostřednictvím elektronického nástroje, jakož i za správnost kontaktních údajů uvedených u účastníka zadávacího řízení zodpovídá účastník zadávacího řízení.

21.4. Komunikace mezi Zadavatelem a dodavatelem v průběhu zadávacího řízení bude probíhat v českém jazyce.

22. Požadavky Zadavatele na zpracování nabídky, způsob podání nabídek a otevírání nabídek

22.1. Účastník předloží úplnou elektronickou verzi nabídky, a to s využitím elektronického nástroje E-ZAK. Způsob správného podání nabídky v elektronické podobě na veřejnou zakázku je uveden v uživatelské příručce elektronického nástroje E-ZAK pro dodavatele, která je k dispozici na internetové stránce profilu zadavatele: <https://zakazky.spravazeleznic.cz/manual.html>.

22.2. Pro tyto účely a v souladu se ZZVZ systém vyžaduje registraci účastníků a elektronický podpis založený na kvalifikovaném certifikátu. Podáním nabídky účastník se stanovenou formou komunikace a doručování souhlasí a zavazuje se poskytnout veškerou nezbytnou součinnost, zejména provést registraci v elektronickém nástroji E-ZAK a pravidelně kontrolovat doručené zprávy.

22.3. Účastník je povinen přiložit ke své nabídce čestné prohlášení o tom, že v souvislosti se zadávacím řízením na předmětnou veřejnou zakázku neuzavřel a neuzavře s jinými osobami zakázanou dohodu ve smyslu zákona č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů. Vzor čestného prohlášení je upraven jako Příloha č. 11 této zadávací dokumentace.

22.4. Pro zpracování nabídky Zadavatel doporučuje níže uvedené řazení dokladů a dokumentů:

- a) Obsah nabídky;
- b) Doklady prokazující splnění základní způsobilosti;
- c) Doklady prokazující splnění profesní způsobilosti;
- d) Doklady prokazující splnění technické kvalifikace;
- e) Vyplněný formulář pro vyplnění nabídkové ceny v souladu s čl. 1414 této zadávací dokumentace;
- f) Vyplněný závazný vzor smlouvy v souladu s čl. 17 této zadávací dokumentace;
- g) Vyplněný dokument „Požadavky na služby Platformy SŽ“ jež tvoří Příloha č. 19 této zadávací dokumentace;
- h) Vyplněný Log management a SIEM dotazník v souladu s čl. 28 této zadávací dokumentace (dodavatel využije Příloha č. 20 této zadávací dokumentace);
- i) Čestné prohlášení ve vztahu k zakázaným dohodám dle čl. 22.3 této zadávací dokumentace (dodavatel využije Příloha č. 11 této zadávací dokumentace);
- j) Čestné prohlášení podle čl. 25.3 této zadávací dokumentace v případě, že účastník v souladu s čl. 25.2 této zadávací dokumentace vyznačí

ve smlouvě části, které jsou předmětem obchodního tajemství nebo ty části, ve kterých jsou obsaženy informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS;

- k) Čestné prohlášení ke střetu zájmů v souladu s čl. 26.2 této zadávací dokumentace;
- l) Čestné prohlášení o splnění podmínek v souvislosti se situací na Ukrajině dle čl. 27.5 této zadávací dokumentace;
- m) V případě využití poddodavatelů seznam poddodavatelů vyhotovený v souladu s čl. 15.1 této zadávací dokumentace.

22.5. Nabídka musí být podána elektronickými prostředky prostřednictvím elektronického nástroje E-ZAK, který je profilem Zadavatele, a to v českém jazyce nebo v souladu s ustanovením § 45 odst. 3 ZZVZ. Zadavatel nepřipouští podání nabídky v listinné podobě ani v jiné elektronické formě mimo elektronický nástroj E-ZAK.

22.6. Nabídky podávané v elektronické podobě účastník doručí do konce níže uvedené lhůty pro podání nabídek, a to prostřednictvím elektronického nástroje E-ZAK na níže uvedenou elektronickou adresu <https://zakazky.spravazeleznice.cz/>.

22.7. Dokumenty musí být do systému E-ZAK vkládány jako jeden soubor (ve výše uvedených formátech) nebo více zkomprimovaných souborů ve formátu zip, rar nebo 7z, bez použití hesla. Zkomprimované soubory nesmí obsahovat žádný další zkomprimovaný soubor. Zadavatel upozorňuje, že systém elektronického zadávání veřejných zakázek E-ZAK umožňuje pracovat se soubory o velikosti nejvýše 50 MB za jeden takový soubor, příp. zkomprimované soubory. Soubory většího rozsahu je nutno před jejich odesláním prostřednictvím E-ZAK vhodným způsobem rozdělit. Velikost samotné nabídky jako celku není nijak omezena.

23. Lhůta pro podání nabídek bude stanovena prostřednictvím elektronického nástroje E-ZAK.

23.1. Lhůta pro podání nabídek bude stanovena prostřednictvím elektronického nástroje E-ZAK.

23.2. Otevírání nabídek je v souladu s § 109 ZZVZ neveřejné, bude probíhat bez přítomnosti účastníků a bude zahájeno bez zbytečného odkladu po uplynutí lhůty pro podání nabídek.

24. Informace pro dodavatele a podmínky pro uzavření smlouvy

24.1. Zadavatel si v souladu s **§ 170 ZZVZ vyhrazuje právo zrušit zadávací řízení.**

24.2. Požadavky Zadavatele pro uzavření smlouvy

24.2.1. Vybraný dodavatel je povinen Zadavateli na písemnou výzvu učiněnou dle § 122 odst. 3 ZZVZ předložit chybějící doklady.

24.2.2. Zadavatel je oprávněn v písemné výzvě dle bodu 24.2.1 zadávací dokumentace určit další doklady, které je vybraný dodavatel povinen předložit v souladu s § 122 odst. 4 ZZVZ, tj. zejména originály nebo úředně ověřené kopie dokladů.

24.2.3. U vybraného dodavatele, je-li českou právnickou osobou, zadavatel zjistí údaje o:

jeho skutečném majiteli podle zákona upravujícího evidenci skutečných majitelů (dále jen „**skutečný majitel**“) z evidence skutečných majitelů podle téhož zákona (dále jen „**evidence skutečných majitelů**“).

Vybraného dodavatele, je-li zahraniční právnickou osobou, zadavatel vyzve k předložení výpisu ze zahraniční evidence obdobné evidenci skutečných majitelů nebo, není-li takové evidence,

a) ke sdělení identifikačních údajů všech osob, které jsou jeho skutečným majitelem, a

b) k předložení dokladů, z nichž vyplývá vztah všech osob podle předchozího písmene a) k dodavateli; těmito doklady jsou zejména:

- výpis ze zahraniční evidence obdobné veřejnému rejstříku,
- seznam akcionářů,
- rozhodnutí statutárního orgánu o vyplacení podílu na zisku,
- společenská smlouva, zakladatelská listina nebo stanovy.

24.2.4. Zadavatel vyloučí vybraného dodavatele, je-li českou právnickou osobou, která má skutečného majitele, pokud nebylo možné zjistit údaje o jeho skutečném majiteli z evidence skutečných majitelů (k zápisu zpřístupněnému v evidenci skutečných majitelů po odeslání oznámení o vyloučení dodavatele se nepřihlíží).

24.2.5. Zadavatel vyloučí vybraného dodavatele, je-li zahraniční právnickou osobou, pokud nepředložil údaje.

24.2.6. Zadavatel upozorňuje, že preferuje uzavírání smluv v elektronické podobě prostřednictvím některého druhu zaručených elektronických podpisů. V případě, že dodavatel není schopen k takovému postupu zajistit Zadavateli součinnost, žádáme, aby Zadavatele o této skutečnosti informoval ve své nabídce, a to v průvodní zprávě k nabídce.

24.3. Další podmínky Zadavatele pro uzavření smlouvy (§ 104 ZZVZ)

24.3.1. Vybraný dodavatel je povinen Zadavateli na písemnou výzvu učiněnou dle § 122 odst. 3 písm. b) ZZVZ předložit doklady a informace dle čl. 26.3 a čl. 27.6 této zadávací dokumentace.

24.3.2. Neposkytnutí uvedené součinnosti vybraným dodavatelem je v souladu s ustanovením § 122 odst. 8 ZZVZ důvodem pro vyloučení vybraného dodavatele.

25. Registr smluv

25.1. Zadavatel je povinen uveřejňovat uzavřené smlouvy v registru smluv na základě ustanovení zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „**ZRS**“).

25.2. Zadavatel na základě výše uvedeného požaduje, aby účastník pro účely uveřejnění smlouvy v registru smluv ve smlouvě, která bude nedílnou součástí nabídky, označil její části, které jsou předmětem obchodního tajemství nebo ty části, ve kterých jsou obsaženy

informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS.

25.3. Pokud účastník ve smlouvě, která bude nedílnou součástí nabídky, označí její části nebo určité informace dle čl. 25.2 této zadávací dokumentace, je účastník povinen předložit Čestné prohlášení. Vzor čestného prohlášení je zpracován jako Příloha č. 12 této zadávací dokumentace. Tímto čestným prohlášením účastník prohlašuje, že jím uvedené údaje a skutečnosti kumulativně naplňují všechny definiční znaky obchodního tajemství tak, jak je vymezeno v ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**obchodní tajemství**“), a pro případ, že by takto označené údaje a skutečnosti nenaplněly znaky obchodního tajemství a takto znečitelněná smlouva by byla v důsledku toho uveřejněna způsobem odporujícím ZRS, nese účastník veškerou odpovědnost.

25.4. Výše uvedené čestné prohlášení dle čl. 25.3 této zadávací dokumentace účastník nedokládá v případě, že neoznačí ve smlouvě, která bude nedílnou součástí nabídky, žádné takové části nebo informace ve smyslu čl. 25.2 této zadávací dokumentace.

25.5. Účastník odpovídá za správnost a pravdivost veškerých údajů a skutečností, které jím budou uvedeny ve výše uvedeném čestném prohlášení. Zadavatel nebude přezkoumávat jejich pravdivost.

25.6. Výjimkou z povinnosti uveřejnění smlouvy v registru smluv jsou důvody uvedené v ustanovení § 3 odst. 2 ZRS. Je-li účastník subjektem uvedeným v ustanovení § 3 odst. 2 písm. k) ZRS (případně je subjektem uvedeným v ustanovení § 3 odst. 2 ZRS dle jiného písmene, než je zde uvedeno), doporučuje Zadavatel, aby účastník tuto skutečnost uvedl v nabídce. V případě, že tak účastník neučiní, bude Zadavatel postupovat, jako by na smlouvu nedopadala výjimka uvedená v ustanovení § 3 odst. 2 písm. k) ZRS (případně jiná výjimka dle ustanovení § 3 odst. 2 ZRS dle jiného písmene, než je zde uvedeno) a zadavatel neodpovídá za škodu nebo jakoukoliv jinou újmu tímto postupem vzniklou.

26. Střet zájmů dle zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů

26.1. Dle § 4b zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „**Zákon o střetu zájmů**“), se nesmí účastnit zadávacích řízení dle ZZVZ jako účastník zadávacího řízení nebo jako poddodavatel, prostřednictvím kterého účastník zadávacího řízení prokazuje kvalifikaci, obchodní společnost, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.

26.2. Zadavatel požaduje, aby dodavatel a jeho poddodavatel, prostřednictvím kterého prokazuje kvalifikaci, nebyli ve střetu zájmů dle § 4b Zákona o střetu zájmů. Skutečnost, že dodavatel a jeho poddodavatel, prostřednictvím kterého prokazuje část kvalifikace, nejsou ve střetu zájmů dle § 4b Zákona o střetu zájmů, prokáže dodavatel předložením čestného prohlášení, jehož vzorové znění je v Příloha č. 13 této zadávací dokumentace, ve své nabídce.

26.3. Vybraný dodavatel je povinen předložit k výzvě Zadavatele dle § 122 odst. 3 písm. b) ZZVZ doklady a informace, z nichž nepochybně vyplýne, že vybraný dodavatel i všichni poddodavatelé, jimiž vybraný dodavatel prokazuje kvalifikaci, splňují podmínku neexistence střetu zájmů ve smyslu § 4b Zákona o střetu zájmů a tohoto čl. 26 této zadávací dokumentace. V případě vybraného dodavatele nebo jeho poddodavatele, prostřednictvím kterého vybraný dodavatel prokazoval část kvalifikace, je-li zahraniční právnickou osobou,

je vybraný dodavatel povinen předložit zejména doklady ve smyslu § 122 odst. 5 ZZVZ, a to i ve vztahu k příslušnému poddodavateli, prostřednictvím kterého vybraný dodavatel prokazoval část kvalifikace.

26.4. V případě postupu účastníka zadávacího řízení v rozporu s čl. 26 této zadávací dokumentace bude účastník zadávacího řízení vyloučen ze zadávacího řízení.

27. Další zadávací podmínky v návaznosti na sankce proti Rusku a Bělorusku v souvislosti se situací na Ukrajině

27.1. Dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů³ (dále jen „**Nařízení č. 833/2014**“) se zakazuje zadat nebo dále plnit jakoukoli veřejnou zakázku nebo koncesní smlouvu spadající do oblasti působnosti směrnic o zadávání veřejných zakázek, jakož i čl. 10 odst. 1, 3, odst. 6 písm. a) až e), odst. 8, 9 a 10, článků 11, 12, 13 a 14 směrnice 2014/23/EU, čl. 7 písm. a) až d), článku 8, čl. 10 písm. b) až f) a h) až j) směrnice 2014/24/EU, článku 18, čl. 21 písm. b) až e) a g až i) a článků 29 a 30 směrnice 2014/25/EU a čl. 13 písm. a) až d), f) až h) a j) směrnice 2009/81/ES a hlavy VII nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 následujícím osobám, subjektům nebo orgánům:

- a. jakémukoli ruskému státnímu příslušníkovi, fyzické osobě s bydlištěm v Rusku nebo právnické osobě, subjektu či orgánu usazenému v Rusku,
- b. právnické osobě, subjektu nebo orgánu, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v písmeni a) tohoto odstavce, nebo
- c. fyzické nebo právnické osobě, subjektu nebo orgánu, které jednají jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b) tohoto odstavce,

včetně subdodavatelů, dodavatelů nebo subjektů, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, pokud představují více než 10 % hodnoty zakázky.

27.2. Zadavatel požaduje, aby účastník zadávacího řízení sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, **nebyli** osobami dle čl. 27.1 této zadávací dokumentace a Nařízení č. 833/2014.

27.3. Dle čl. 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů (dále jen „**Nařízení č. 269/2014**“), a dalších prováděcích předpisů k tomuto Nařízení č. 269/2014 (**tzv. sankční seznamy**)⁴, nesmějí být žádné finanční prostředky ani hospodářské zdroje

³ Zejm. Nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, a Nařízení Rady (EU) 2023/427 ze dne 25. února 2023, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině.

⁴ Zejm. Prováděcí nařízení Rady (EU) 2022/581 ze dne 8. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, prováděcí

přímo ani nepřímo zpřístupněny fyzickým nebo právnickým osobám, subjektům či orgánům nebo fyzickým nebo právnickým osobám, subjektům či orgánům s nimi spojeným uvedeným v příloze I Nařízení nebo v jejich prospěch (dále jen „**Osoby vedené na sankčních seznamech**“).

27.4. Zadavatel dále požaduje, aby účastník zadávacího řízení sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, **nebyli** Osobami vedenými na sankčních seznamech.

27.5. Splnění zadávacích podmínek stanovených Zadavatelem dle tohoto článku prokáže účastník zadávacího řízení předložením čestného prohlášení, jehož vzorové znění je Příloha č. 14 této zadávací dokumentace, ve své nabídce.

27.6. Zadavatel je oprávněn ověřovat si splnění zadávacích podmínek dle tohoto článku. Vybraný dodavatel je povinen předložit k výzvě Zadavatele dle § 122 odst. 3 písm. b) ZZVZ doklady a informace, z nichž nepochybně vyplýne, že vybraný dodavatel i všichni poddodavatelé nebo jiné osoby, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, splňují podmínky uvedené v tomto článku zadávací dokumentace.

27.7. V případě postupu účastníka zadávacího řízení v rozporu s čl. 27 této zadávací dokumentace bude účastník zadávacího řízení vyloučen ze zadávacího řízení.

nařízení Rady (EU) 2022/658 ze dne 21. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny a prováděcí nařízení Rady (EU) 2023/429 ze dne 25. února 2023, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny.

28. Log management a SIEM dotazník

28.1. Dodavatel je povinen vyplnit Log management a SIEM dotazník, který tvoří Příloha č. 20 této zadávací dokumentace (dále jen „**Log management a SIEM dotazník**“), a tento předložit ve své nabídce.

28.2. Dodavatel není oprávněn činit změny či doplnění v Log management a SIEM dotazníku, vyjma údajů, u nichž vyplývá z jejich obsahu povinnost doplnění.

28.3. Dodavatel v Log management a SIEM dotazníku na listu „LM&SIEM“ vyplní ve sloupci D, a to formou Ano/Ne, zda jím nabízené řešení naplňuje požadavek, resp. požadavky, které jsou vymezeny ve sloupci C, a dále pak dodavatel ve sloupci E slovně popíše způsob naplnění daného požadavku (tj. požadavku uvedeného ve sloupci C). Požadavky uvedené na listu „LM&SIEM“ představují závazné požadavky, které musí dodavatelem nabízené řešení vždy splňovat, jinak nebudou naplněny zadávací podmínky Veřejné zakázky.

28.4. Dodavatel dále v Log management a SIEM dotazníku na listu „Licence“ vyplní ve sloupci C názvy jím nabízených (tj. dle dodavatelem nabízeného řešení) licencí, údržby licencí a subskripce licencí, jejichž druh je specifikován ve sloupcích A a B, a dále ve sloupci D dodavatel vyplní počet jím nabízených licencí, subskripce licencí včetně údržby a technické podpory na 60 měsíců nabízené dodavatelem podle sloupce C.

28.5. Dodavatel je povinen Log management a SIEM dotazník doplněný dle výše uvedených pokynů učinit součástí nabídky. Nepředložení vyplněného Log management a SIEM dotazníku v nabídce bude mít za následek vyloučení účastníka ze zadávacího řízení. Vyplnění sloupce D v listu „LM&SIEM“ v Log management a SIEM dotazníku slovem „ne“ bude bráno jako nesplnění zadávacích podmínek, v důsledku čehož bude účastník ze zadávacího řízení vyloučen.

Přílohy Zadávací dokumentace

Příloha č. 1. Bližší specifikace předmětu plnění veřejné zakázky (technická specifikace)

Příloha č. 2. Analýza prostředí – Architektura prostředí SŽ

Příloha č. 3. Analýza prostředí – Popis prostředí sítě UAS

Příloha č. 4. Platforma 2.0

Příloha č. 5. Harmonogram plnění

Příloha č. 6. Závazný vzor smlouvy

Příloha č. 7. Čestné prohlášení o splnění technické kvalifikace – seznam významných služeb

Příloha č. 8. Seznam členů realizačního týmu

Příloha č. 9. Formulář pro vyplnění nabídkové ceny

Příloha č. 10. Dohoda o ochraně důvěrných informací

Příloha č. 11. Čestné prohlášení ve vztahu k zakázaným dohodám

Příloha č. 12. Čestné prohlášení ve vztahu k zákonu o registru smluv

Příloha č. 13. Čestné prohlášení o střetu zájmů

Příloha č. 14. Čestné prohlášení o splnění podmínek v souvislosti se situací na Ukrajině

Příloha č. 15. Vzor seznamu poddodavatelů

Příloha č. 16. Čestné prohlášení ke splnění základní způsobilosti

Příloha č. 17. Výsledky PTK

Příloha č. 18. Interní předpis Zadavatele „Provozní politika prvků v působnosti systému řízení bezpečnosti informací“

Příloha č. 19. Požadavky na služby Platformy SŽ

Příloha č. 20. Log management a SIEM dotazník

Příloha č. 21. Zdroje logů 2023 – 05

Bc. Jiří Svoboda, MBA

generální ředitel

Klasifikace: Veřejný dokument



Technická specifikace

Příloha č. 1 zadávací dokumentace pro zadávací řízení „Log management a SIEM“

Obsah

1	Seznam zkratk	3
2	Úvod	5
2.1	Záměr SŽ v oblasti systému Log management a SIEM	5
2.2	Předmět plnění veřejné zakázky	6
2.3	Etapy a výstupy aktivity	7
2.3.1	Etapa 1	7
2.3.2	Etapa 2	8
2.3.3	Etapa 3	8
2.3.4	Etapa 4	9
2.3.5	Etapa 5	10
2.3.6	Etapa 6	10
2.4	Parametry požadovaného řešení	11
2.4.1	Testovací prostředí	12
2.4.2	Infrastruktura pro přenos logů	12
2.4.3	Řešení vysoké dostupnosti	13
2.4.4	Zálohování	14
2.4.5	Architektura úložišť	14
2.4.6	Provozní monitoring	15
2.4.7	Zabezpečení	15
2.4.8	Log management	15
2.4.9	SIEM	16
2.4.10	Lokality určené k provozu komponent Log management a SIEM	18
2.4.11	Požadavky na technické funkcionality řešení	18
2.4.12	Požadavky na specifikaci virtualizačních prostředků Zadavatele	19
2.4.13	Dodávka hardwarových a softwarových prostředků	20
2.5	Oblasti, které nejsou předmětem plnění veřejné zakázky	20
3	Současný stav a popis prostředí	22
4	Požadavky na plnění	23
4.1	Jednorázové projektové činnosti	23
4.1.1	Před-implementační analýza	23
4.1.2	Instalace a konfigurace řešení	24
4.1.3	Napojení určených zdrojů logů	24
4.1.4	Tvorba a optimalizace bezpečnostní / detekční politiky řešení	25

4.1.5	Školení	26
4.2	Průběžné služby dodavatele řešení	26
4.2.1	Technická podpora servisního týmu SŽ	26
4.2.2	Údržba řešení	27
4.2.3	Konzultace a rozvojové aktivity	28
5	Akceptační milníky	29

1 Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

Zkratka	Popis
API	Rozhraní pro programování aplikací (Application Programming Interface)
CDP	Centrální dispečerské pracoviště
DNS	Systém správy doménových jmen, slouží k převodu jmenných záznamů na adresy informačních systémů a evidenci dalších podpůrných informací
EPS	Jednotka určující objem logů za sekundu v počtu událostí
GB/d	Jednotka určující objem logů za den v Giga Byte
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
HA	Režim vysoké dostupnosti (High Availability), např. prostřednictvím redundance
HTTP	HTTP (Hypertext Transfer Protocol) je internetový protokol určený pro komunikaci s WWW servery
IOC	Indikátor kompromitace (Indicator of Compromise, IOC) je ve forenzním světě důkaz, který v kybernetickém prostředí naznačuje, že došlo k narušení kybernetické bezpečnosti
IS/ICT	Informační systémy a informační a komunikační technologie.
JSON	JavaScript Object Notation je způsob zápisu dat nezávislý na počítačové platformě, určený pro přenos dat, která mohou být organizována v polích nebo agregována v objektech
LM	Log management
MD	Člověkodenní, pracovní čas jedné osoby odpovídající jednomu pracovnímu dni, tedy typicky 8 hodin (man-day)
On-premise	On-premise software je takový software, který lze instalovat a provozovat v prostorách organizace, která jej využívá
OS	Operační Systém
OT	Operational technology (OT) je hardware a software, který zjišťuje nebo způsobuje změny prostřednictvím přímého monitorování a/nebo řízení průmyslových zařízení, prostředků, procesů a událostí.
RAT	Remote Access Tool – druh škodlivého kódu, který umožňuje vzdálené ovládání napadeného systému
SATA	Počítačová sběrnice, která využívá datové rozhraní pro připojení velkokapacitních paměťových zařízení (např. pevných disků)

SIEM	Security Information and Event Management je systém pro správu bezpečnostních informací a událostí.
SLA	Dohoda o úrovni poskytovaných služeb (Service Level Agreement)
SOC	Kybernetické bezpečnostní dohledové centrum.
SSD	Solid-State Drive
SW	Software
SŽ	Správa železnic, státní organizace
SŽT	Správy železniční telematiky
Účastník	Subjekt, který se v rámci tohoto zadávacího řízení uchází o realizaci veřejné zakázky
URL	Uniform Resource Locator (URL), označovaný jako webová adresa, je odkaz na webový zdroj, který určuje jeho umístění v počítačové síti a mechanismus jeho vyhledávání
USB	Univerzální sériové rozhraní informačního systému
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů
WAN	Wide Area Network je v informatice počítačová síť, která pokrývá rozlehlé geografické území
XML	Extensible Markup Language je obecný značkovací jazyk, který byl vyvinut a standardizován konsorciem W3C
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávacího řízení pro výběr dodavatele veřejné zakázky „Log management a SIEM“ (dále jen „veřejná zakázka“), pro organizaci Správa železnic, státní organizace (dále jen „SŽ“). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

2.1 Záměr SŽ v oblasti systému Log management a SIEM

Jedním z požadavků vyplývajících z § 22 VoKB (*Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů*) je požadavek na sběr informací o provozních a bezpečnostních činnostech a jejich ochranu před neoprávněným přístupem nebo změnou. V současné době jsou informace o provozních a bezpečnostních událostech (logy) zaznamenávány převážně jen na lokální úrovni, kde není vždy možné zaručit jejich integritu a bezpečí.

Cílem aktivity je zavést kompletní řešení pro centrální sběr a uchovávání informací o provozních a bezpečnostních událostech (logů), zaručujícím jejich integritu i všechny další požadavky kladené výše uvedenou VoKB. Toho by mělo být dosaženo nasazením centrálního log management řešení a zapojením potřebných zdrojů logů ze systémů a sítě SŽ do tohoto řešení.

Aktivita definuje implementaci systému správy logů a SIEM jako jeden z kroků zaměřujících se na zlepšení celkového stavu zabezpečení organizace (SŽ). Jedním z hlavních očekávání je zlepšit detekci hrozeb a čas potřebný k reakci tím, že se umožní monitorování a analýza logů z různých systémů v téměř reálném čase. To povede nejen ke zlepšení detekce hrozeb, ale také k rychlejší reakci v případě bezpečnostního incidentu.

Klíčovým cílem je také zajištění souladu s příslušnými bezpečnostními standardy, které se v organizaci (SŽ) uplatňují. Zavedením systému pro správu logů a SIEM chce organizace (SŽ) sledovat a vykazovat bezpečnostní události, a tím zajistit soulad s takovými normami.

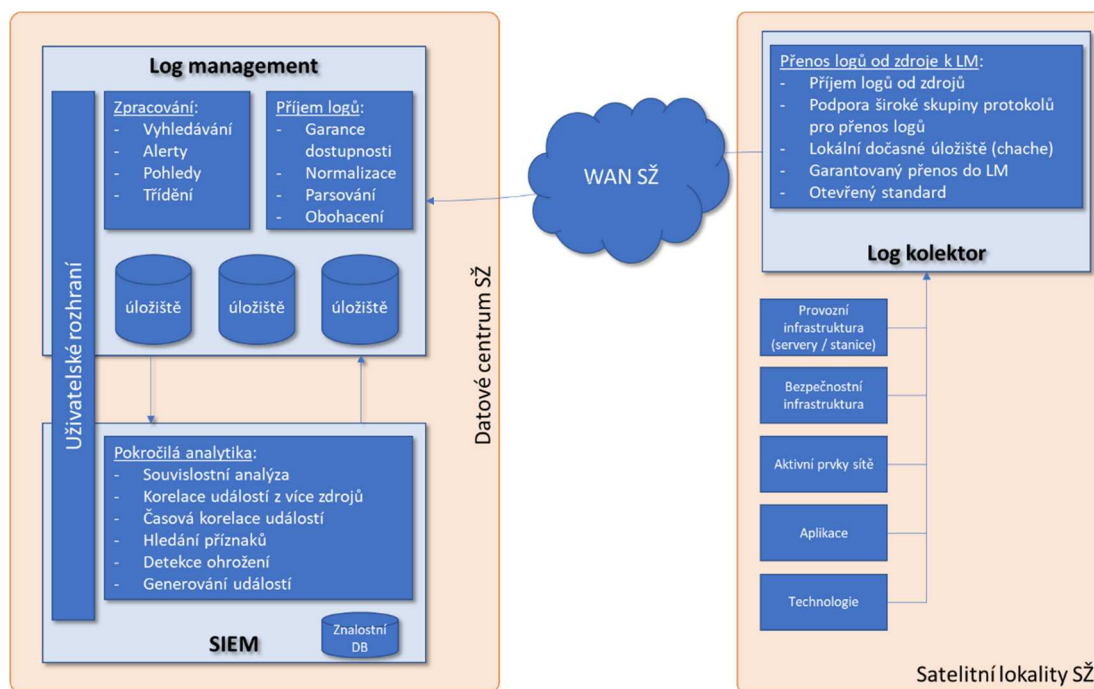
Zavedení systému správy logů a SIEM také zefektivní vyšetřování incidentů. Centralizované úložiště logů, které požadované řešení poskytne, umožní bezpečnostním týmům rychle a efektivně vyšetřovat zachycené bezpečnostní i provozní incidenty.

Dalším cílem implementace systému správy logů a SIEM je snížení provozních nákladů a požadavků na součinnosti. Automatizovaný sběr a analýza logů sníží manuální úsilí potřebné k vyšetřování a hlášení bezpečnostních incidentů, čímž se sníží provozní náklady. Kombinace těchto cílů umožní organizaci (SŽ) posílit její bezpečnostní pozici, zvýšit efektivitu a snížit náklady, čímž se systém správy logů a SIEM stane důležitou součástí komplexní strategie kybernetické bezpečnosti.

2.2 Předmět plnění veřejné zakázky

Předmětem aktivity je řešení Log management a SIEM, které bude zajišťovat jednotný sběr provozních a bezpečnostních událostí z prostředí SŽ, uchovávat je pro potřeby analýzy a archivovat je v souladu s legislativními požadavky (zejména s požadavky dle § 22 VoKB). Součástí SIEM, která je bezpečnostní nadstavbou nad systémem Log management, bude zajišťovat detekci provozních a bezpečnostních událostí, které je možné odvodit od struktury, posloupnosti a významu zaznamenaných logů, nebo na základě předem definovaných symptomatických pravidel.

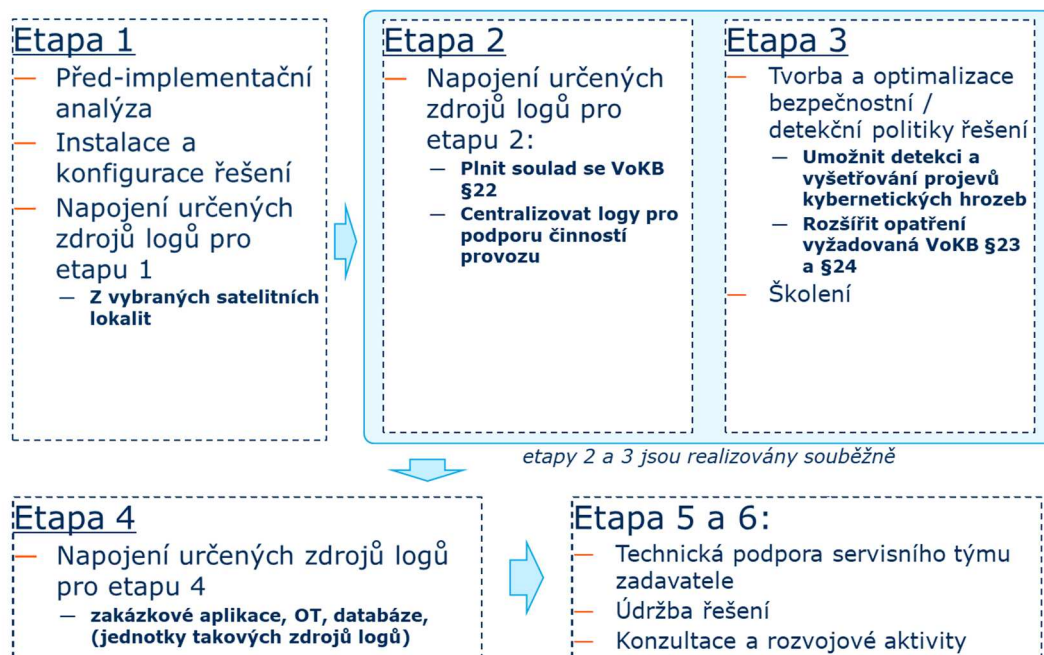
Řešení je požadováno realizovat v režimu „centralizovaném“, tedy všechny logy budou přenášeny infrastrukturou SŽ na jedno centrální místo. Přenos bude realizován soustavou log kolektorů, které budou zajišťovat sběr logů od zdrojů logů a dle definovaných pravidel je předají do centrálního úložiště. Přenos logů musí být realizován spolehlivým způsobem, tedy bez ztrát logů, jejich nechtěné modifikace nebo vyzrazení.



Jednotlivé komponenty řešení budou muset umožňovat a dle požadovaných parametrů také poskytovat vysokou dostupnost. Očekáváním od vysoké dostupnosti je, že nebudou narušeny nezbytné funkcionality řešení a tím omezena možnost užívání řešení nebo porušeny zákonné a regulatorní povinnosti.

2.3 Etapy a výstupy aktivity

Aktivita Log management a SIEM bude rozdělena do jednotlivých etap, které zajistí postupnou realizovatelnost, specifikaci dílčích milníků a finanční plnění vůči dodavateli. Všechny etapy budou součástí jediné veřejné zakázky a budou jen dílčím rozdělením činností.



2.3.1 Etapa 1

V první části bude zajištěna realizace řešení pro přenos, uložení a interpretaci logů z provozní a bezpečnostní infrastruktury SŽ. Dále bude provedena instalace komponenty SIEM a všech vyžadovaných prvků vysoké dostupnosti. Pro potvrzení funkcionality první etapy, bude požadováno napojení vzorových zdrojů logů, které budou vybrány jako reprezentativní z vybraných satelitních lokalit (Brno, Plzeň) i centrální lokality (Praha U2 / CDP Praha). Zdroje logů pro tuto etapu jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05“ a označeny ve sloupci „Priorita napojení“ příslušnou etapou, během níž bude vyžadováno jejich napojení.

Aktivita	Popis aktivity
Před-implementační analýza	<i>Popisuje způsob a podmínky nasazení technologie Log management a SIEM do prostředí SŽ.</i>
Instalace a konfigurace řešení	<i>Budou dodány všechny nezbytné softwarové komponenty řešení, potřebný hardware a licence výrobců software.</i> <i>Funkční řešení pro sběr, ukládání, vyhodnocování logů. Funkční systém pro řešení garantovaného přenosu logů infrastrukturou SŽ. Funkční rozhraní pro práci s nástrojem, vyhledávání logů a jejich interpretaci.</i>
Napojení určených zdrojů logů pro etapu 1	<i>Napojení logů z vybraných satelitních lokalit pro ověření funkční přenosové trasy od zdroje logu k systému Log management.</i> <i>Napojení logů z vybraných zdrojů k ověření výkonnostních parametrů a schopnosti řešení užívat a ovládat.</i>

2.3.2 Etapa 2

Tato etapa bude zaměřena na napojování všech zdrojů logů, které budou uvedeny jako zdroje logů podmiňující akceptaci díla. Tyto logy dodavatel napojí na připravené kolektory logů, zajistí jejich transport do centrálních komponent řešení Log management, připraví a nasadí všechny parsovací a normalizační politiky, aby logy byly uloženy v požadovaném formátu umožňujícím jejich další využití. Zdroje logů pro tuto etapu jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05“ a označeny ve sloupci „Priorita napojení“ příslušnou etapou, během níž bude vyžadováno jejich napojení.

Aktivita	Popis aktivity
Napojení určených zdrojů logů pro etapu 2	<i>Dodavatel, se součinností SŽ, zajistí napojení všech určených zdrojů logů, čímž prokáže schopnost nástroje zpracovat všechny druhy logů, které SŽ pro tuto etapu specifikovala.</i>

2.3.3 Etapa 3

V této etapě bude vytvořena konfigurace pro vyhodnocování logů v komponentě SIEM, pravidla pro detekce symptomů v lozích a korelační pravidla. Výstupní generované události budou předávány na určené odběratele, kteří budou specifikováni v rámci přípravy před-implementační analýzy. Tato etapa bude realizována souběžně s etapou 2 a nebude se vyčkávat na dokončení napojení všech zdrojů logů definovaných pro celé dílo.

Aktivita	Popis aktivity
Tvorba a optimalizace bezpečnostní / detekční politiky řešení	<p><i>Dodané komponentě SIEM bude definován způsob nakládání s logy – tento způsob bude dodavatelem nastaven a bude ověřena jeho funkčnost.</i></p> <p><i>Nad logy, které jsou již zasílány do systému Log managementu, bude dodavatelem vytvořena sada detekčních a korelačních pravidel, kterými budou naplněny požadavky na USE-CASES SŽ, které jsou uvedeny na listu „USE-CASES“ v příloze č. 21 zadávací dokumentace.</i></p> <p><i>Nad nastavenými detekcemi budou vytvořena pravidla pro integraci se systémy SŽ, jako např. JIRA, MS Teams. Důležité je, aby byla naplněna potřeba SŽ o předávání detekovaných událostí jejich zamýšleným odběratelům, tedy útvarům SOC a provoz SŽT.</i></p>
Školení pracovníků SŽ	<p><i>Pracovní týmy SŽ budou vyškoleny v:</i></p> <ul style="list-style-type: none"> - <i>administraci řešení</i> - <i>technické podpoře řešení</i> - <i>napojování zdrojů logů</i> - <i>práci s logy (hledání, třídění, interpretaci)</i> - <i>práci v nástroji SIEM</i> - <i>tvorbě detekčních a korelačních politik.</i>

2.3.4 Etapa 4

Etapa bude obsahovat připojování specifických vzorových zdrojů logů (jednotky množství zdrojů) u nichž je očekávána potřeba specifické úpravy nastavení komponent řešení. Mezi taková specifika patří zejména vybraná aktiva z technologických částí sítí, specifické aplikační zdroje logů a podobné. Zdroje logů pro tuto etapu jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05“ a označeny ve sloupci „Priorita napojení“ příslušnou etapou, během níž bude vyžadováno jejich napojení.

Aktivita	Popis aktivity
Napojení určených zdrojů logů pro etapu 4	<p><i>SŽ vybere specifické zdroje logů, které dodavatel v této etapě připojí. Bude se jednat o napojení logů zakázkových aplikací, vybraných zařízení z prostředí OT a databázových systémů.</i></p> <p><i>Bude se jednat o jednotky takových systémů, jejichž napojením dodavatel prokáže flexibilitu řešení a možnosti, jak řešit napojení nestandardních zdrojů logů.</i></p> <p><i>SŽ bude schopno další zdroje logů napojovat ve vlastní režii, jen s možností čerpání technické podpory dodavatele řešení.</i></p>

2.3.5 Etapa 5

Aktivita	Popis aktivity
Technická podpora servisního týmu SŽ	<i>Technická podpora dodaného řešení a provoz Help Desku dodavatele.</i>
Údržba řešení	<i>Zajištění pravidelné údržby všech komponent dodaného řešení, a to včetně bezpečnostní údržby.</i>

2.3.6 Etapa 6

Aktivita	Popis aktivity
Konzultace a rozvojové aktivity	<i>Rozvojové aktivity, které budou souviset především ve změnami v prostředí SŽ, které mohou mít dopad na provoz řešení Log management a SIEM.</i>

2.4 Parametry poptávaného řešení

Všechny komponenty řešení požaduje SŽ provozovat v režimu on-premise (tedy výhradně na zařízení v infrastruktuře SŽ). Přípustná integrace s online / CLOUD službami je pouze pro aktualizací služby a získávání informací o hrozbách. Není přípustné předávat data z prostředí SŽ ke zpracování k výrobci nabízeného řešení, pokud tuto aktivitu manuálně (a pouze pro konkrétní vyšetřování) neinicuje pracovník SŽ.

Řešení Log management a SIEM je poptáváno jako ucelené softwarové řešení, které obsahuje veškeré potřebné licence k naplnění poptávaných parametrů řešení, včetně technické podpory (maintenance nebo subscribe) výrobce nabízených komponent řešení a technické podpory dodavatele řešení, a to na dobu 5 let.

Technická podpora dodavatele bude řízena dle parametrů uvedených ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT Zadavatele (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně ustanovením kapitoly „12. SERVISNÍ MODEL“. SŽ požaduje plnění v parametrech servisního modelu „B1 Závažný“.

SŽ požaduje provoz Help Desku dodavatele, který bude provozován v režimu odpovídajícím specifikaci uvedené ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT Zadavatele (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně ustanovením kapitoly „10. HELPDESK“. SŽ požaduje plnění Help Desku v režimu „Režim 1“ a úrovni „L3“.

Parametr	Jednotka	Hodnota
Celkem událostí za vteřinu	EPS	40000
Celkový denní objem logů	GB/d	1000
Počet lokalit pro umístění log kolektorů	počet	16
Celkový počet lokalit pro umístění centrálních komponent: <ul style="list-style-type: none"> - Jedná se o dvě pracoviště v rámci Prahy - Lokality jsou propojeny silným datovým propojem - SŽ chce využít lokalit pro geo-redundanci centrálních komponent řešení 	počet	2

Minimální doba, po kterou budou logy v systému Log management uloženy	měsíců	18
---	--------	----

2.4.1 Testovací prostředí

SŽ požaduje dodání řešení včetně testovacího prostředí, které bude obsahovat všechny komponenty řešení, licencované na nejmenší dostupné objemy, popřípadě opatřené přímo licenci pro testovací účely. Testovací prostředí musí disponovat prvky režimu vysoké dostupnosti, z důvodu možnosti jejich testování, bude však provozováno pouze v centrálním datovém centru. Testovací prostředí bude sloužit zejména k ověřování nových konfigurací, testování procesů aktualizace SW, řešení chybových stavů apod.

Pro napojení na testovací prostředí jsou vybrány jednotky zdrojů logů, které jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05“ vyplněním údaje „ANO“ ve sloupci „Testovací prostředí“.

2.4.2 Infrastruktura pro přenos logů

SŽ požaduje, aby přenos logů od jednotlivých zdrojů logů do centrálních komponent řešení Log management a SIEM, bylo říditelné, zajištěno bezpečným způsobem a řešení bylo otevřené případnému napojování jiných centrálních komponent řešení.

2.4.2.1 Podpora zdrojů logů

Přenosovou infrastrukturu požaduje SŽ realizovat takovým nástrojem, který umožní integraci se zdroji logů, které jsou uvedeny v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05“, a to formou:

1. Pasivního příjmu logů, kdy log odesílá zdroj logu a využívá komunikačních protokolů:
 - a. SYSLOG (TCP/UDP)
 - b. HTTP/HTTPS
 - c. SNMP Trap
 - d. TCP
 - e. UDP
 - f. WEF (Windows Event Forwarder)
2. Aktivního vyčítání logů ze zdrojového systému:
 - a. Office 365 Services
 - b. Office 365 Activity
 - c. Office 365 Message Trace
 - d. Kafka
 - e. Azure Event Hubs
 - f. Azure Blob Storage
 - g. Soubor na lokální / vzdáleném souborovém systému
 - h. Databázový systém (SQL)

Zdroje logů z prostředí Microsoft systémů, které umožní předávání prostřednictvím Windows Event Forwarder, budou tento způsob využívat. Prostor Windows Event Forwarder bude ve správě SŽ.

2.4.2.2 Dostupné parametry nastavení řešení

Řešení pro přenos logů musí umožnit nastavení filtračních pravidel, kterými bude možné již před přenosem logů do centrálních komponent řešení, nastavit filtrační pravidla pro redukci objemů přenášených logů (např. odfiltrování logů nepodstatných pro kybernetickou bezpečnost) dle jejich typu, kategorie nebo klíčových slov.

Dalším požadavkem na konfiguraci řešení je možnost upravovat parametry dočasné paměti (cache / buffer), kterou bude možné využívat k uložení logů od zdrojových systémů v případě nedostupnosti cílových centrálních komponent řešení. Požadavek na kapacitu této dočasné paměti je 5 dnů, pokud nebude v před-implementační analýze rozhodnuto o snížení této hodnoty. Po obnovení dostupnosti centrálních komponent řešení budou uložené logy odeslány spolehlivým a bezpečným způsobem, tedy tak, že přenos bude šifrovaný a uložení logů do centrálních komponent řešení bude potvrzováno (k vyprázdnění dočasné paměti dojde až po potvrzení uložení na centrálním úložišti).

Přenášené logy budou komprimovány, aby byl optimalizován dopad na přenosovou infrastrukturu SŽ.

2.4.2.3 Bezpečnost řešení

SŽ vyžaduje, aby všechna spojení mezi satelitními kolektory a centrálními komponentami probíhalo zabezpečeně pomocí šifrování a ochrany integrity, přičemž kryptografické algoritmy budou zabezpečeny v souladu s aktuálními doporučeními NÚKIB dle článku 20.15. Zvláštních obchodních podmínek pro zakázku v oblasti ICT (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace).

2.4.2.4 Otevřenost řešení

Dodané řešení pro přenos logů od zdrojů logů do centrálních komponent řešení musí podporovat otevřené komunikační standardy (alespoň SYSLOG, SNMP Trap, Kafka, TCP JSON, ELASTICSEARCH, souborový systém), kterými bude zajišťováno spojení s nástrojem Log management a SIEM. SŽ nepřipouští, aby tato spojení byla realizovatelná pouze proprietárním komunikačním protokolem výrobce řešení Log management a SIEM.

2.4.3 Řešení vysoké dostupnosti

Vysoká dostupnost je vyžadována u centrálních komponent Log management a SIEM, přičemž SŽ požaduje, aby dodavatel navrhl takové řešení, které splní minimálně následující podmínky:

1. Management rozhraní pro práci s logy a pro analýzu událostí bude provozováno v režimu vysoké dostupnosti Active-Standby nebo Active-

Active a jednotlivé komponenty budou rozloženy mezi 2 datová centra SŽ, která jsou určena k provozu centrálních komponent řešení.

2. Úložiště logů a vygenerovaných událostí (alertů) bude provozováno v režimu vysoké dostupnosti Active-Standby nebo Active-Active, přičemž všechna data musejí vždy existovat alespoň ve dvou replikách, kdy každá z replik bude vždy jedna v každém ze 2 datových center SŽ, která jsou určena k provozu centrálních komponent řešení.

2.4.4 Zálohování

SŽ požaduje dodání řešení včetně návrhu způsobu zálohování jednotlivých komponent řešení, přičemž minimálně budou požadovány následující parametry:

1. Konfigurace všech komponent řešení budou zálohovány v pravidelném cyklu minimálně 1 x denně.
2. Aplikační prostředí všech komponent řešení budou zálohována v pravidelném cyklu minimálně 1 x denně.
3. Bezpečnostní události (aletry a auditní logy Log management a SIEM), které vygenerují nástroje Log management a SIEM, budou zálohovány v pravidelném cyklu minimálně 1 x denně.
4. Data logů, která budou v nástroji Log management uloženy, nebudou podléhat potřebě zálohování – SŽ počítá s dostatečnou odolností dat v rámci jejich rozložení do úložišť ve 2 datových centrech SŽ. Řešení musí umožnit export vybraných logů (vybraných dle zdroje a typu logu) k provedení jejich zálohy na externí zálohovací zařízení SŽ.

2.4.5 Architektura úložišť

Systém Log management musí podporovat rozklad diskové kapacity na různá úložiště s různou úrovní přístupnosti a rychlosti, která jsou známa jako úložiště HOT, WARM a COLD. Tento přístup, který se často nazývá víceúrovňová architektura úložiště (tiered storage architecture) a umožňuje efektivní správu a ukládání logů s ohledem na jejich důležitost a aktuálnost.

1. Úložiště HOT: Toto úložiště je určeno pro okamžité a intenzivní zápisy logů. Jedná se o nejrychlejší a nejdražší úložiště SSD (Solid-State Drive). Logy, které jsou často přístupné a které vyžadují rychlý přístup, budou ukládány na úložišti HOT.
2. Úložiště WARM: Úložiště WARM slouží pro ukládání logů, které již nejsou tak často přístupné jako na úložišti HOT, ale stále mají určitou důležitost a potřebují být uchovávány pro analýzu, výzkum nebo případnou kontrolu. Toto úložiště je provozováno na discích s nižší rychlostí přenosu dat, jako je SATA disk.
3. Úložiště COLD: Úložiště COLD je určeno pro ukládání starých a méně důležitých logů, které jsou přístupné jen zřídka. Tato data ukládáme na pomalejších a levnějších médiích, jako jsou pásková úložiště.

Při využití víceúrovňové architektury úložiště se Log management systémy často spoléhají na různé mechanismy, jako je automatizované přesouvání logů mezi

úložišti na základě jejich věku, důležitosti nebo jiných kritérií. To umožňuje optimalizaci využití diskové kapacity a uchování logů s ohledem na jejich hodnotu a přístupnost.

SŽ vyžaduje, aby nabízené řešení umožňovalo na aplikační úrovni rozlišování druhů úložišť pro:

1. HOT úložiště, která jsou specifická tím, že jejich stáří od doby uložení do Log management není delší než 3 měsíce
2. WARM úložiště budou všechna ostatní data až do požadovaného období pro uložení 18 měsíců.

Využití úložiště úrovně COLD bude sloužit pouze pro účely archivace / zálohování vybraných druhů logů (viz. kapitola „Zálohování“ této Technické specifikace) a bude dostupné pouze v lokalitách SŽ určených pro provoz centrálních komponent řešení.

2.4.6 Provozní monitoring

SŽ provozuje nástroj provozního monitoringu ZABBIX a požaduje, aby součástí dodávky byl také soupis doporučených dohledovaných parametrů a hodnot nabízeného řešení pro zajištění monitoringu operačních systémů a aplikačního prostředí dodávaného řešení. Cílem je předcházet provozním incidentům na všech komponentách Log management a SIEM, včetně všech komponent dodaných pro přenos logů od zdroje logu až po centrální komponenty.

2.4.7 Zabezpečení

Dodávané řešení a všechny jeho komponenty budou splňovat bezpečnostní doporučení výrobce (tzv. hardening) a svou vlastní konfigurací umožní dodržení souladu s požadavky ZokB, resp. VoKB a jejich kapitol:

- § 18 Bezpečnost komunikačních sítí [písmena c) a d)]
- § 19 Správa a ověřování identit [odstavce 3, 5 písm. a) a 6 písm. a)]
- § 20 Řízení přístupových oprávnění
- § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů [odstavce 2 písm. d) a 2 písm. e)]
- § 26 Kryptografické prostředky [písmena a), c) a d)].

2.4.8 Log management

Kybernetické bezpečnostní řešení Log management pro SŽ s centralizovanou architekturou by mělo splňovat následující požadavky:

1. Shromažďování logů: Řešení musí umožňovat shromažďování logovacích dat z různých zdrojů v organizaci (SŽ), včetně síťových prvků, serverů, aplikací a vybraných koncových zařízení.
2. Centralizace: Veškeré logy musí být sbírány a ukládány v centrálním datovém centru. Centralizovaná architektura umožňuje snadnou správu a

analýzu dat a zajišťuje jednotný pohled na logovací informace z celé organizace.

3. Škálovatelnost: Řešení musí být schopné zvládat velké množství logovacích dat v rozsáhlé organizaci. Musí být navrženo tak, aby bylo schopné efektivně zpracovávat a ukládat logy ze všech specifikovaných satelitních lokalit (kapitola „2.4.10 Lokality určené k provozu komponent Log management a SIEM“ této Technické specifikace).
4. Bezpečnostní funkce: Log management řešení musí obsahovat bezpečnostní funkce, jako je šifrování dat při přenosu, ověřování identity uživatelů systému, kontrola a řízení přístupu. To zajistí ochranu logovacích dat proti neoprávněnému přístupu a manipulaci.
5. Real-time monitoring: Řešení musí poskytovat možnost sledování logovacích událostí v reálném čase. To umožní rychlou detekci a odpověď na bezpečnostní incidenty. Požadovaná vlastnost může být sdílenou součástí se SIEM vrstvou.
6. Vyhledávání a dotazování: Řešení musí poskytovat efektivní nástroje pro vyhledávání a dotazování logovaných dat. To umožní snadnou analýzu a vyhledávání specifických informací v rozsáhlých datových sadách.
7. Reporting a vizualizace: Řešení musí poskytovat možnosti tvorby reportů a vizualizace logovacích dat. To umožní vytváření přehledných reportů a grafů, které usnadní prezentaci a analýzu logovacích informací pro bezpečnostní tým, provoz a popř. i management.
8. Auditovatelnost: Řešení musí splňovat požadavky na auditovatelnost, což zahrnuje sledování a záznam veškerých aktivit týkajících se logování i analýzy dat a auditovatelnost aktivit privilegovaných uživatelů systému Log management. To je důležité pro dodržování regulací a standardů v oblasti kybernetické bezpečnosti.
9. Rozšiřitelnost: Log management řešení musí být navrženo tak, aby bylo snadno rozšiřitelné a přizpůsobitelné rostoucím potřebám organizace (SŽ). To zahrnuje možnost přidávat nové zdroje logů a rozšiřovat kapacitu systému bez výrazného poklesu výkonu.

Celkově řečeno, kybernetické bezpečnostní řešení Log managementu s centralizovanou architekturou by mělo SŽ umožňovat efektivní shromažďování, analýzu, sledování a ochranu logovacích dat z různých zdrojů v celé organizaci (SŽ). Splnění těchto požadavků pomůže organizaci (SŽ) zlepšit svou schopnost detekovat, reagovat a předcházet kybernetickým hrozbám a incidentům a vyhovět požadavkům vyplývajícím ze ZoKB a VoKB.

2.4.9 SIEM

Nedílnou součástí požadovaného řešení je také komponenta SIEM (Security Information and Event Management), která poskytne rozšířené funkcionality pro analýzu bezpečnostních událostí a monitorování hrozeb. Kybernetické

bezpečnostní řešení SIEM pro SŽ s centralizovanou architekturou by mělo splňovat následující požadavky:

1. **Detekce a analýza hrozeb:** SIEM řešení musí poskytovat pokročilou detekci a analýzu bezpečnostních hrozeb. To zahrnuje monitorování aktivit a událostí v reálném čase, vyhledávání anomálií, identifikaci známých indikátorů kompromitace (IOC) a podporu pro vyhledávání souvislostí mezi různými událostmi.
2. **Korelace událostí:** Funkce pro korelaci událostí je klíčovou součástí SIEM řešení. Tímto způsobem lze identifikovat spojitosti a vzorce mezi různými událostmi a aktivitami v prostředí. To umožňuje identifikovat sofistikované hrozby a předcházet jim dříve, než způsobí větší škody.
3. **Pravidla a upozornění:** SIEM musí umožňovat vytváření pravidel a upozornění pro rychlou identifikaci a reakci na bezpečnostní události. Administrátoři by měli mít možnost definovat specifická pravidla a podmínky, na jejichž základě systém vygeneruje upozornění na potenciální bezpečnostní incidenty.
4. **Integrace s Log managementem:** SIEM musí být plně integrované s nabízeným Log management řešením. Tím se zajišťuje, že logy z různých zdrojů jsou k dispozici pro analýzu a monitorování bezpečnostních událostí a zároveň poskytuje holistický pohled na bezpečnostní situaci organizace (SŽ). Toto však neznamená, že všechny logy uložené v prostředí Log management budou zpracovávány komponentou SIEM. SŽ požaduje, aby bylo možné licenčně rozlišit data ukládaná jen v Log management a data, která budou určena ke zpracování v komponentě SIEM.
5. **Vizualizace a reporting:** SIEM řešení by mělo poskytovat možnosti vizualizace dat a tvorby reportů. To umožňuje uživatelům snadno sledovat a analyzovat bezpečnostní události prostřednictvím interaktivních grafů, tabulek a dashboardů. Reporty pak umožňují prezentaci důležitých informací managementu a auditům.
6. **Sledování souladu:** SIEM by měl poskytovat funkcionalitu pro sledování souladu s příslušnými bezpečnostními předpisy, normami a regulacemi, jako je například GDPR, ZoKB. Tím se organizaci (SŽ) umožní dodržování požadovaných standardů a předpokladů v oblasti ochrany dat a informací.
7. **Rozšiřitelnost a výkon:** SIEM by měl být navržen s ohledem na vysokou škálovatelnost a výkon. To umožní efektivní zpracování velkých objemů dat a událostí, které vznikají v rozsáhlých a dynamických prostředích SŽ.

SIEM řešení s centralizovaným Log managementem by mělo poskytovat pokročilé funkce pro detekci, analýzu a monitorování bezpečnostních událostí. Integrace s existujícími nástroji, vizualizace dat, správa incidentů a podpora souladu s regulacemi jsou další klíčové aspekty, které budou zohledněny při výběru SIEM řešení.

2.4.10 Lokality určené k provozu komponent Log management a SIEM

Typ lokality	Adresa lokality	Účel
CDP	V Trianglu 2474, Praha 9	Centrální komponenty LM / SIEM
Datové centrum	Pod Táborem 369/8a, Praha 9	Centrální komponenty LM / SIEM
Datové centrum	Kulkova 1, Brno (Maloměřice)	Satelitní log kolektor
Datové centrum	Škroupova 1017/11, Plzeň	Satelitní log kolektor
Datové centrum /CDP	Tovární 3286, Přerov	Satelitní log kolektor
Oblastní ředitelství	ATU, Ostrava	Satelitní log kolektor
Oblastní ředitelství	Kounicova 26, Brno	Satelitní log kolektor
Oblastní ředitelství	Pávovská 2, Jihlava	Satelitní log kolektor
Oblastní ředitelství	Křížíkova 552, Praha 1	Satelitní log kolektor
Oblastní ředitelství	Pernerova 2819/2a, Praha 2	Satelitní log kolektor
Oblastní ředitelství	Riegrovo náměstí 1660, Hradec Králové	Satelitní log kolektor
Oblastní ředitelství	ATU, Pardubice	Satelitní log kolektor
Oblastní ředitelství	Sušická 1168/23, Plzeň	Satelitní log kolektor
Oblastní ředitelství	A. Trägers 2899/90, České Budějovice	Satelitní log kolektor
Oblastní ředitelství	Železničářská 1386/31, Ústí nad Labem	Satelitní log kolektor
Organizační jednotka	Kounicova 26, Brno	Satelitní log kolektor
Organizační jednotka	Nerudova 773/1, Olomouc	Satelitní log kolektor
Technologická / sdělovací místnost	Wilsonova 300/8, Praha 2	Satelitní log kolektor
Technologická / sdělovací místnost	Havlíčková 1011, Praha 1	Satelitní log kolektor

2.4.11 Požadavky na technické funkcionality řešení

Všechny parametry požadované v tomto dokumentu a přílohách zadávací dokumentace jsou pro dodavatele závazné a SŽ vyžaduje jejich naplnění.

Požadavky na vybrané funkcionality poptávaného řešení, které SŽ vyžaduje splnit technickými prostředky, a u nichž Účastník musí popsat způsob, kterým jím nabízené řešení naplní požadavek, jsou specifikovány v přiloženém dotazníku „Log management a SIEM dotazník“, který je Přílohou č. 20 zadávací dokumentace;

v tomto dotazníku Účastník potvrdí připravenost nabízeného řešení splnit vybrané požadavky a vyplní způsob, kterým je každý požadavek naplněn. Účastník do přiloženého dotazníku doplní také soupis všech licencí nabízeného řešení, kterým zajistí naplnění požadovaných funkcionalit.

SŽ upozorňuje, že nesplnění kteréhokoliv požadavku na technické funkcionality řešení uvedeného v přiloženém dotazníku, povede k vyloučení Účastníka ze zadávacího řízení. V případě, že bude nesplnění takového požadavku odhaleno až v průběhu realizace plnění, bude to považováno za hrubé porušení povinností dle přílohy č. 6 zadávací dokumentace – Závazného vzoru smlouvy a bude důvodem pro odstoupení od této smlouvy.

2.4.12 Požadavky na specifikaci virtualizačních prostředků Zadavatele

V souvislosti se schválenou strategií IS/ICT SŽ, konkrétně cílem zajištění dlouhodobého koncepčního a efektivního rozvoje IS/ICT, požaduje SŽ využití možností jeho hardwarové a virtualizační platformy pro jednotlivé komponenty poptávaného řešení. Popis platformy je uveden v příloze č. 4 zadávací dokumentace, která je označena jako „Platforma SŽ 2.0“.

Pro veškeré prostředky, ve všech lokalitách určených k provozu řešení Log management a SIEM, které je možné provozovat v platformě SŽ, vyplní Účastník specifikaci technických požadavků na platformu SŽ, a to do připraveného listu „Požadavky“ v Příloze č. 19 zadávací dokumentace, která je označena jako „Požadavky na služby Platformy SŽ pro Log Management a SIEM“.

Jedná se zejména o následující parametry:

- Požadovaný počet kusů daného řešení
- Požadovaný počet Core
- Požadovaná velikost RAM
- Požadovaná velikost diskového prostoru na úložišti typu COLD storage
- Požadovaná velikost diskového úložiště v úložišti typu HOT/WARM storage
- Požadovaná velikost diskového úložiště pro zálohování (BACKUP).

Náklady na rozšíření virtualizační platformy SŽ do požadovaných parametrů, nebude Účastník uvádět jako součást nabídkové ceny, tedy do svých nákladů. SŽ bude hodnotit nároky nabízeného řešení na virtualizační platformu pomocí bodovacího systému, na základě celkového požadovaného výpočetního výkonu uvedeného v listu „Požadavky“, který je součástí Přílohy č. 19 zadávací dokumentace.

SŽ limituje celkové požadavky na výpočetní výkon a kapacitu, který je připraven pro účely projektu nabídnout, takto:

**Parametr výkonu a
kapacity**

Maximální povolená hodnota

Počet v CPU	1046
Kapacita RAM (GB)	4877
Kapacita disků (GB)	1860000

2.4.13 Dodávka hardwarových a softwarových prostředků

Výjimkou, kdy není nutné využití platformy SŽ, jsou samozřejmě komponenty řešení, které virtualizaci neumožňují. V takovém případě uvede dodavatel veškeré náklady na hardware, který je součástí dodávaného řešení a nebude provozován v platformě SŽ, do své cenové kalkulace a učiní jej součástí své dodávky.

Pokud bude součástí nabízeného řešení také dodávka technických a programových prostředků, bude Účastník respektovat, že:

Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) na základě ZoKB Varování, č. j. 3012/2018NÚKIB-E/110, kde uvedl, že: *„Použití technických nebo programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:*

- *Huawei Technologies Co., Ltd, Šen-čen, Čínská lidová republika*
- *ZTE Corporation, Šen-čen, Čínská lidová republika“.*

Dne 4. ledna 2019 vydal NÚKIB Metodiku k varování ze dne 17. prosince 2018 (dále jen „metodika“), kde jsou mj. určeny i postupy pro aktualizaci analýzy rizik. V souladu s vydanou metodikou provedla SŽ analýzu rizik související s předmětnou veřejnou zakázkou na dodávky, jak je jeho povinností podle § 5 a § 8 VOKB. V návaznosti na to SŽ identifikovala rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná, a současně opatření k jejich zvládnutí, kterým je nepřipouštění použití těchto prostředků v rámci plnění veřejné zakázky.

SŽ tak na základě varování NÚKIB, navazující metodiky a provedené analýzy rizik, ve spojení s § 4 odst. 4 ZoKB, nepřipouští v rámci plnění veřejné zakázky použití technických nebo programových prostředků společností (výrobců), které jsou uvedené v současné době platném varování NÚKIB jako hrozba v oblasti kybernetické bezpečnosti.

2.5 Oblasti, které nejsou předmětem plnění veřejné zakázky

- Instalace a správa virtualizační platformy, která zajišťuje prostor pro provoz komponent řešení Log management a SIEM.

- Instalace a správa operačních systémů, které jsou součástí nabízených instancí virtualizační platformy SŽ, pokud dodavatel nebude vyžadovat instalaci specifického OS, nebo provádění zásahů do standardní instalace.
- Provozní monitoring HW a virtualizačního prostředí SŽ, které zajišťuje provoz jednotlivých komponent řešení Log management a SIEM.
- Úprava a konfigurace zdrojů logů pro účely jejich integrace na komponenty řešení Log management a SIEM.
- Provoz archivačního systému pro dlouhodobé uložení logů mimo prostředí řešení Log management a SIEM.

3 Současný stav a popis prostředí

Současný stav ICT prostředí SŽ je popsán v příložených dokumentech:

- Analýza prostředí – architektura prostředí SŽ (Příloha č. 2 zadávací dokumentace)
- Analýza prostředí – popis prostředí sítě UAS (Příloha č. 3 zadávací dokumentace)
- Platforma 2.0 - souhrn podporovaných infrastrukturních služeb, technologií, a architektonických principů, která definuje základní rámec pro návrh řešení ICT (Příloha č. 4 zadávací dokumentace)

4 Požadavky na plnění

SŽ očekává dodávku komplexního řešení, která se bude sestávat z jednorázových projektových činností, dodávky nástroje se souvisejícími technickými komponenty a průběžných služeb dodavatele řešení.

4.1 Jednorázové projektové činnosti

Jednorázové projektové činnosti jsou nedílnou součástí dodávaného řešení, jsou zahrnuty mezi akceptační milníky a je k nim vázána etapizace dodávky a fakturace.

4.1.1 Před-implementační analýza

Před-implementační analýza	
Popis	<p>Před-implementační analýza popisuje způsob a podmínky nasazení technologie Log management a SIEM do prostředí SŽ. Dokument musí popisovat charakteristiku dodávaného technického řešení, popis jednotlivých jeho komponent, navrhovaný způsob zapojení do prostředí SŽ a samozřejmě způsob integrace zdrojů logů.</p> <p>Dokument musí mít charakter detailní technické specifikace pro všechny uvažované implementační postupy, na jejichž předběžném schválení závisí umožnění provádět technické zásahy do prostředí SŽ.</p>
Výstupy	<p>Výstupem tohoto kroku bude dokument obsahující alespoň:</p> <ul style="list-style-type: none"> • Popis dodávaného technického řešení a jeho komponent • Návrh architektury dodávaného řešení v prostředí SŽ • Detailní popis implementačních kroků • Detailní technická specifikace <ul style="list-style-type: none"> ◦ Umístění technologií ◦ Napájení ◦ Síťové segmenty pro správu technologie ◦ IP adresace ◦ HW požadavky na virtualizační platformu SŽ ◦ Požadavky na síťové přístupy ◦ Požadavky na přístup do internetu ◦ Požadavky na vzdálený přístup pro správu technologie ◦ Požadavky na systémový monitoring ◦ Postup napojení zdrojů logů do Log management / SIEM • Revizi USE-CASES, které jsou uvedeny v listu „USE-CASES“ v příloze č. 21 zadávací dokumentace, zadaných v rámci TS a doporučení dalších USE-CASES dodavatelem • Požadované součinnosti na SŽ • Návrh akceptačních testů • Katalog projektových rizik a návrh způsobu jejich ošetření • Specifikace kroků, součinností dodavatele a jejich rozsah v MD, při ukončení projektu (exit plán), které budou součástí poskytované služby

- Detailní harmonogram implementace řešení

4.1.2 Instalace a konfigurace řešení

	Instalace a konfigurace řešení
Popis	V této části projektu dojde k dodání, instalaci a konfiguraci všech komponent technického řešení Log management a SIEM, které naplní požadavky předmětu veřejné zakázky a naplní specifika projektu uvedená v dokumentu před-implementační analýza.
Výstupy	<p>Výstupem tohoto kroku bude funkční technické řešení Log management a SIEM, které bude:</p> <ul style="list-style-type: none"> • Obsahovat všechny potřebné licence, předplatné a technické podpory výrobce. • Dodáno s nezbytným hardwarem pro komponenty, které není vhodné provozovat ve virtuálním prostředí SŽ. • Nasazeno na všech požadovaných lokalitách pro etapu 1 včetně komponent pro přenos logů od zdroje do centrálních úložišť. • V souladu se schválenou architekturou. • Zcela funkční pro výkon funkce Log management a SIEM, tak jak SŽ požaduje v této Technické specifikaci. • Napojeno na systémový monitoring SŽ (systém Zabbix). • Schopno vyhovět definovaným akceptačním testům v rozsahu specifikovaným v před-implementační analýze a schváleným SŽ.

4.1.3 Napojení určených zdrojů logů

	Napojení určených zdrojů logů
Popis	V této části projektu dojde k napojení určených zdrojů logů, které SŽ určila k napojení do prostředí Log management a SIEM pro odpovídající etapu projektu. Zdroje logů jsou zvlášť specifikovány pro etapu 1, etapu 2 a etapu 4 v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05“ uvedením odpovídající etapy ve sloupci „Priorita napojení“.
Výstupy	<p>Výstupem tohoto kroku bude funkční napojení zdroj logů na Log management a SIEM a bude obsahovat:</p> <ul style="list-style-type: none"> • Nasazení komponent infrastruktury pro přenos logů ze satelitních lokalit do centrálních úložišť řešení (nad rámec komponent instalovaných v etapě 1). • Provedení technické integrace se zdrojem logu <ul style="list-style-type: none"> ◦ Výběr komunikačního protokolu ◦ Výběr typů logových zpráv. • Nastavení přenosové platformy pro zajištění garantovaného odeslání logů od zdrojového systému k centrálním prvkům řešení Log management a SIEM.

- Ověření přenosu logů od zdroje do centrálního úložiště.
- Nastavení zpracování logů od zdrojů pro podporu další datové analýzy (parsing).
- Nastavení normalizace logů, pokud je to vyžadováno řešením pro naplnění požadavků uvedených v technické specifikaci a požadavcích na detekční USE-CASES, které jsou uvedeny v listu „USE-CASES“ v příloze č. 21 zadávací dokumentace.
- Nastavení retenční politiky pro logy.

4.1.4 Tvorba a optimalizace bezpečnostní / detekční politiky řešení

	Tvorba a optimalizace bezpečnostní / detekční politiky řešení
Popis	V této části projektu bude dodavatelem provedeno vyhodnocení účinnosti nasazeného řešení Log management a SIEM, bude upravena bezpečnostní / detekční pravidla a zdokumentovány všechny provedené konfigurační úpravy, které vedou k vyšší efektivitě detekce kybernetických bezpečnostních událostí pro analytický tým SOC SŽ.
Výstupy	<p>Výstupem tohoto kroku bude funkční technické řešení Log management a SIEM, které bude mít upravenou bezpečnostní / detekční politiku tak, že bude minimalizován objem falešných detekcí, které by musel analytický tým SOC zpracovávat. SŽ požaduje provedení alespoň následujících činností:</p> <ul style="list-style-type: none"> • Zohlednění reálných dostupných IP adresací SŽ v detekčních politikách. • Upřesnění konkrétních druhů validních aktiv SŽ zaznamenaných v komunikacích, které jsou důležité pro fungování detekčních pravidel (DNS, SMTP, WEB, NTP, PROXY, MS AD). • Vytvoření specifických detekčních politik (tzv. detekčních use-cases), dle specifikace SŽ, které jsou specifikovány v příloze č. 21 zadávací dokumentace „Zdroje logů - 2023-05.“ v listu „USE-CASES“. • Aplikace výjimek, které doporučí SŽ. • Předávání detekovaných událostí jejich odběratelům, kterými budou pracoviště SOC, nebo provozní tým SŽT. <p>Všechny upravené konfigurace budou zdokumentovány a předány jako výstup této části projektu.</p>

4.1.5 Školení

	Školení
Popis	V této části projektu bude dodavatelem provedeno zaškolení technického servisního týmu SŽ a týmu Security Operations Center SŽ. Cílem je přenesení znalostí o správě dodaných nástrojů a předání rutinní správy na tým SŽ. Druhé specifické školení by se mělo hlouběji zaměřit na školení práce s řešením Log management a SIEM, jehož odběratelem bude pracoviště SOC SŽ.
Výstupy	<p>Výstupem tohoto kroku bude realizované školení se zaměřením na využívání a správu technického řešení Log management a SIEM:</p> <ul style="list-style-type: none"> • Prezenční školení servisního týmu SŽ. SŽ nominuje 8 pracovníků a bude požadovat naplnění časové dotace alespoň 3 MD. <ul style="list-style-type: none"> ◦ komponenty systému ◦ konfigurační parametry komponent ◦ ladění výkonnostních a kapacitních parametrů řešení ◦ troubleshooting ◦ update a upgrade. • Prezenční školení týmu SOC SŽ v prostorách výrobce zakončené certifikací účastníků. SŽ nominuje 4 pracovníky a bude požadovat naplnění časové dotace alespoň 3 MD. <ul style="list-style-type: none"> ◦ zaměření na užívání nástroje Log management a SIEM ◦ tvorba a úprava detekčních pravidel ◦ vyšetřování a analýza událostí ◦ aktivní vyhledávání kybernetických hrozeb.

4.2 Průběžné služby dodavatele řešení

4.2.1 Technická podpora servisního týmu SŽ

	Technická podpora servisního týmu zadavatele
Popis	<p>Technická podpora bude řízena dle parametrů uvedených ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT SŽ (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně v ustanovení kapitoly „12. SERVISNÍ MODEL“. SŽ požaduje plnění v parametrech servisního modelu „B1 Závažný“.</p> <p>SŽ požaduje provoz Help Desku dodavatele, který bude provozován v režimu odpovídajícím specifikaci uvedené ve Zvláštních obchodních podmínkách pro zakázky v oblasti ICT SŽ (Příloha č. 7 Závazného vzoru smlouvy, který je Přílohou č. 6 zadávací dokumentace), konkrétně v ustanovení kapitoly „10. HELPDESK“. SŽ požaduje plnění Help Desku v režimu „Režim 1“ a úrovni „L3“.</p>
Výstupy	Výstupem tohoto bude poskytnutí služby dle parametrů požadovaných SŽ a definovaných v servisní smlouvě s dodavatelem.

4.2.2 Údržba řešení

	Údržba řešení
Popis	<p>Dodavatel zajistí pravidelnou údržbu všech komponent dodaného řešení, a to včetně bezpečnostní údržby. Cílem je, aby byl zajištěn provoz řešení v aktuální verzích produktu, které budou považovány za stabilní a bezpečné.</p> <p>Dodavatel zajistí aplikaci výrobcem vydávaných opravných balíčků, nových funkcionalit a bezpečnostních záplat.</p> <p>Průběžně prováděné a pravidelné činnosti zahrnují (prováděné min. 1x měsíčně):</p> <ul style="list-style-type: none"> • Aktivní sledování a využívání nových postupů v oblasti zabezpečení systémů a komunikací. • Průběžné aplikování bezpečnostních oprav od výrobců. • Udržování aktuálnosti SW verzí dodaného řešení, a to minimálně v režimu aktuální MAJOR verze a MINOR verze ne starší než 2 vydání. Případné výjimky musí schválit SŽ. • Sběr podkladů pro aktualizaci dokumentace / evidence aktiv SŽ. • Pravidelná profylaxe systémových prostředků systému, včetně návrhu řešení nalezených problémů nebo rozvoje systému. • Kontrola provozních systémových logů s následným řešením případných incidentů. • Kontrola funkčnosti a bezpečnosti úložiště hesel. • Vypracování protokolu o údržbě s detailním popisem veškerých nalezených nedostatků a postupu pro jejich odstranění.
Výstupy	Výstupem tohoto bude poskytnutí služby dle parametrů požadovaných SŽ.

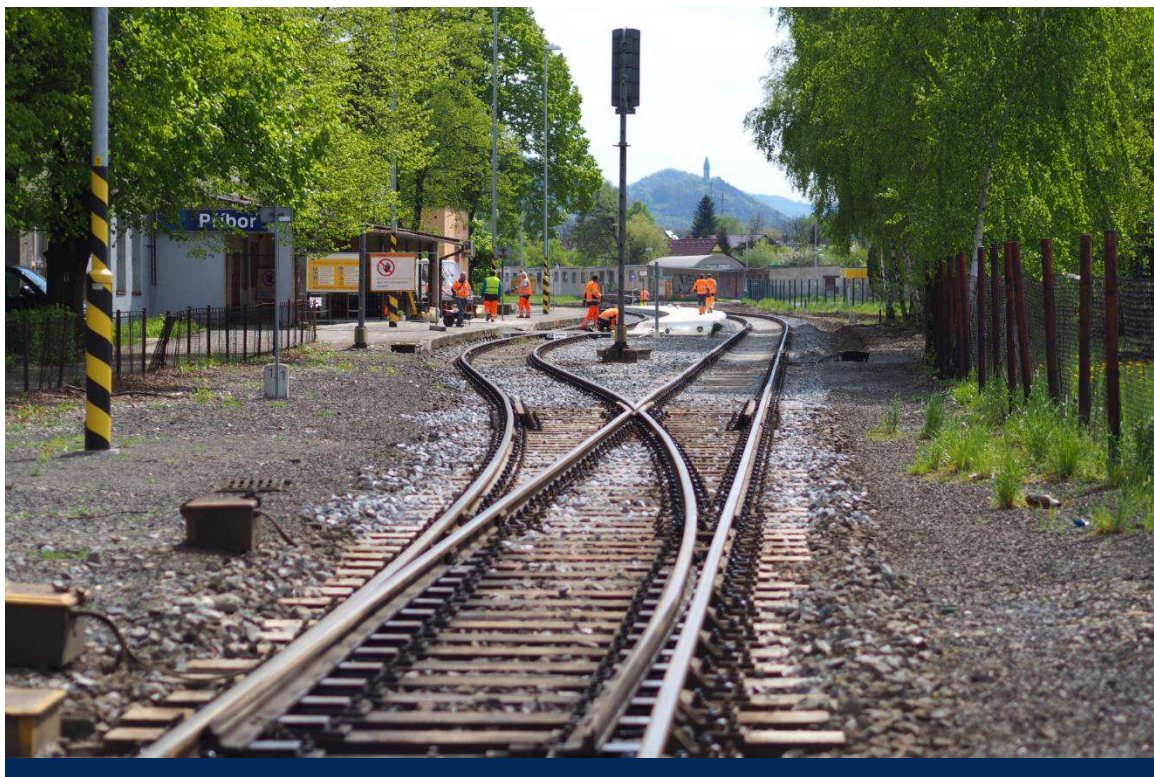
4.2.3 Konzultace a rozvojové aktivity

	Konzultace a rozvojové aktivity
Popis	<p>Dodavatel poskytne SŽ služby konzultace na vyžádání. Maximální souhrn těchto služeb bude činit 250 MD za celou dobu trvání smlouvy, čerpání bude probíhat dle konkrétních potřeb SŽ. Jedná se o rozvojové aktivity, které budou souviset především s:</p> <ul style="list-style-type: none"> - změnami v prostředí SŽ, které mohou mít dopad na provoz řešení Log management a SIEM. - integrací prostředí Log management a SIEM na procesy Security Operations Center <ul style="list-style-type: none"> o Incident Response o Forezní analýza o Sběr IoC. - pokročilou analýzou dat. - zajištěním udržitelnosti prostředí Log management a SIEM.
Výstupy	Výstupem tohoto bude poskytnutí služby konzultace na vyžádání podle potřeb SŽ.

5 Akceptační milníky

Plnění musí být dodáno v níže uvedených etapách. Každá z níže uvedených etap (tj. každý řádek níže uvedené tabulky) musí být SŽ separátně akceptována nejpozději v termínu uvedeném v harmonogramu. SŽ akceptuje výstupy dané Etapy, jestliže je dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentaci této veřejné zakázky.

Etapa	Popis	Kapitola obsahující požadavky
Etapa 1A	Jednorázové projektové činnosti: - Před-implementační analýza	4.1.1
Etapa 1B	Jednorázové projektové činnosti: - Instalace a konfigurace řešení - Napojení určených zdrojů logů pro etapu 1	4.1.2 4.1.3
Etapa 2	Jednorázové projektové činnosti: - Napojení určených zdrojů logů pro etapu 2	4.1.3
Etapa 3	Jednorázové projektové činnosti: - Tvorba a optimalizace bezpečnostní / detekční politiky řešení - Školení	4.1.4 4.1.5
Etapa 4	Jednorázové projektové činnosti: - Napojení určených zdrojů logů pro etapu 4	4.1.3
Etapa 5	Průběžné služby dodavatele řešení: - Technická podpora servisního týmu SŽ - Údržba řešení	4.2.1 4.2.2
Etapa 6	Průběžné služby dodavatele řešení: - Konzultace a rozvojové aktivity	4.2.3



Platforma SŽ 2.0: Vymezení služeb

Březen 2022

Historie verzí

Verze	Popis	Platnost od	Předchozí verze
1.0	Úvodní verze Platformy SŽ	27.01.2020	
2.0	Aktualizace Platformy SŽ s názvem „Platforma SŽ 2.0: Vymezení služeb“	01.04.2022	

Obsah

Seznam zkratk	4
1 Úvod	5
2 Platforma Správy železnic	6
3 Motivace Platformy SŽ	7
4 Architektonické principy	8
5 Služby Platformy SŽ	10
5.1 Infrastrukturní služby	10
5.1.1 Služba virtuálních strojů	10
5.1.2 Služba datového uložení	10
5.2 Platformní služby	11
5.2.1 Služba zabezpečeného portálového řešení	11
5.2.2 Služby zabezpečených webových serverů	11
5.2.3 Služby zabezpečených aplikačních serverů	11
5.2.4 Služby zabezpečených databázových prostředí	11
5.3 Podpůrné služby	12
5.3.1 Bezpečnost	12
5.3.2 Monitoring, alerting	12
5.3.3 Aktualizace systémů, Distribuce aplikací	12
5.3.4 Zálohování	12
5.3.5 Komunikační infrastruktura	13
6 Technologie Platformy SŽ	14
7 Přílohy	16

Seznam zkratek

APP	Aplikační vrstva
AS	Aplikační server
AU	Archivní úložiště
DB	Databáze
DR	Disaster Recovery
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
OS	Operační systém
SW	Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost
SŽ	Správa železnic, státní organizace
SŽT	Správa železničních informačních technologií
VM	<i>z angl. „Virtual Machine“</i> . Virtuální stroj
WLS	WebLogic Server
WS	Webový server
ZZVZ	Zákon o zadávání veřejných zakázek

1 Úvod

Cílem tohoto dokumentu je definovat Platformu SŽ, jakožto souhrn podporovaných infrastrukturních služeb, technologií, a architektonických principů, která definuje základní rámec pro návrh řešení ICT. Platforma SŽ naplňuje strategické cíle IS/ICT SŽ, zejména v oblasti efektivního provozu a rozvoje ICT prostředí Správy železnic.

2 Platforma Správy železnic

Platforma Správy železnic definuje prostředí, které standardizuje a podporuje návrh, implementaci a provozování veškerého ICT řešení pro Správu železnic. Popisuje infrastrukturní a platformní služby, podporované technologie a upravuje pravidla jejich použití. Primárním cílem Platformy SŽ je poskytnout potenciálním dodavatelům přehled o prostředí SŽ a současně umožnit organizaci SŽ zajištění efektivního vytváření a provozování ICT řešení při dodržení vysoké kvality a bezpečnosti služeb.

Dokument je udržován a pravidelně aktualizován jednotkou SŽT.

Platforma SŽ obsahuje:

- Architektonické principy SŽ
- Katalog služeb Platformy SŽ
- Katalog technologií Platformy SŽ

Při plánování a rozšiřování ICT řešení je nutné respektovat všechny části Platformy SŽ.

Navíc v případech zakázkového vývoje software pro SŽ musí dodavatel splnit požadavky definované v dokumentu Standardy vývoje informačních systémů SŽ, který je přílohou tohoto dokumentu.

3 Motivace Platformy SŽ

Cílem Správy železnic je zajistit, že:

- Uchazeči výběrových řízení na ICT řešení budou hodnoceni na základě jejich celkové ekonomické efektivity, a nikoliv pouze na základě nabídkové ceny,
- Externí dodávky ICT řešení budou koncepčně a technologicky zapadat do celopodnikového prostředí Správy železnic,
- Dodávané řešení bude možné bezpečně a ekonomicky efektivně provozovat v krátko-, středně-, i dlouhodobém časovém horizontu,
- Provozované technologie SŽ budou perspektivní, moderní a bezpečné,
- Technologická různorodost prostředí SŽ bude:
 - na jednu stranu dostatečně široká, aby neúměrně neomezovala soutěž potenciálních dodavatelů, a
 - na druhou stranu dostatečně ohraničená, aby umožnila efektivní správu systémů zaměstnanci a dodavateli SŽ.

Platforma SŽ je motivovaná schválenou strategií IS/ICT SŽ, a to konkrétně cílem *zajištění dlouhodobého koncepčního rozvoje IS/ICT a jeho souladu se strategickými cíli SŽ, a to zavedením řízení celopodnikové IS/ICT architektury*¹.

Očekává se, že tento dokument pomůže s nastavením jasných povinných parametrů pro nové uchazeče v oblasti technologických standardů SŽ.

Mezi přínosy dokumentu Platformy SŽ 2.0 patří:

- Nastavení společných (minimálních/maximálních) úrovní vyspělosti jednotlivých technologií napříč IS/ICT SŽ a postupné omezení velkých rozdílů v úrovních používaných technologií.
- Stanovení architektonických a technologických standardů pro tvůrce systémů a pro uchazeče o dodávku IS/ICT pro SŽ.
- Zajištění standardizace technických prostředků.
- Zajištění ochrany předchozích investic.
- Zajištění možnosti bezpečného převzetí systémů do provozu a zajištění provozu interními silami SŽ.

¹ Strategie IT a ICT Správy železnic (157463/2021-SŽ-GR-SŽT)

4 Architektonické principy

Kapitola stanovuje základní rámec pravidel a principů, které je nutné respektovat při návrhu a realizaci ICT řešení podle Platformy SŽ.

P01: Bezpečnost a soulad s vnitropodnikovými předpisy

- Navrhované řešení a procesy jím podporované musí být v souladu s legislativními a regulatorními nároky a vnitropodnikovými předpisy Správy železnic.
- Řešení musí umožnit monitorování akcí uživatelů, zejména jejich práce s daty a dokumenty.
- Musí být zajištěna administrovatelnost a auditovatelnost integračních vazeb.
- Vývoj a test není realizován na produkčním prostředí.
- Topologie a architektura produkčního a testovacího prostředí musí být identická, odlišovat se může ve výkonu a použitých zdrojích.
- Před nasazením do produkčního prostředí je řešení prokazatelně otestováno.
- Nejsou realizovány integrace mezi produkčními a neprodukčními prostředími.
- Dohled je zajištěn na všech vrstvách řešení (HW, OS, DB, AS, aplikace, koncový uživatel).
- Musí být zajištěno napojení na centrální dohledovou konzoli.
- Služby poskytované do prostředí internetu budou procházet penetračním testem.

Zdůvodnění: Bezpečnost umožňuje chránit hodnoty Správy železnic. Ve SŽ je nutné udržovat vysokou míru bezpečnosti, a to především v oblastech, které mohou mít dopady na lidské životy. Navrhovaná řešení také musí být nezbytně v souladu s Vyhláškou č. 82/2018 Sb.o Kybernetické bezpečnosti.

P02: Provozovatelnost řešení

- Řešení je provozovatelné na službách a technologiích Správy železnic.
- Řešení musí umožňovat převzetí do provozního prostředí Správy železnic
- Řešení umožňuje škálování.

Zdůvodnění: Z důvodu snahy o udržitelnost provozu je stanoven udržitelný počet technologií, které jsou spolehlivé a mají perspektivu svého rozvoje. Aplikace provozovaná na takto definované skupině technologií tak může být v případě potřeby převzata do provozu a spravována týmem IT specialistů SŽ, jež disponuje patřičnými znalostmi, případně vlastní příslušné certifikace, aby mohli tyto technologie či systémy spravovat. Tím dochází nejen ke zvýšení produktivity, ale také k časové a finanční úspoře, především z pohledu lidských zdrojů.

P03: Znovupoužitelnost řešení

- Řešení musí umožňovat logické oddělení dat pro současné využívání funkcionality různými subjekty (tzv. multitenant).
- V rámci Správy železnic se realizuje minimalizace počtu a rozsahu používaných technologií a aplikací.
- Snižováním počtu a rozsahu používaných technologií a aplikací snižujeme komplexitu správy technologického a aplikačního portfolia.
- Řešení je navrhované s opakováním ověřených jednoduchých návrhových vzorů a designových principů.
- Nasazování změn a nových řešení je seskupováno dle funkcionalit a cílových systémů do jednotlivých „release“. Termíny releasů jsou stanoveny jednotkou SŽT.
- Nasazované řešení nesmí ke svému provozu vyžadovat pravidelný nutný zásah administrátora (např. restarty, čištění logů, ...)

Zdůvodnění: V rámci Správy železnic usilujeme o minimalizaci počtu prostředí pro stejnou funkcionalitu. Znovupoužitelná řešení vedou k úspoře lidských, finančních, časových i materiálních zdrojů v životním cyklu celého řešení.

P04: Nezávislost na dodavatelích

- Řešení je navrhované s ohledem na omezení či eliminaci rizika vendor-lock.

- U řešení převzatých do provozu je cíl převzetí schopnosti vytvořit build aplikace bez závislosti na dodavateli.
- Usilujeme o právo zásahu do zdrojových kódů a rozvoje řešení interními kapacitami Správy železnic nebo dalšími dodavateli. Výjimku mohou tvořit jen případy, kdy by takové požadavky byly ekonomicky výrazně nevýhodné nebo je důvod se domnívat, že tato práva budou nadbytečná.

Zdůvodnění: Nebýt závislí na malém počtu dodavatelů umožňuje SŽ být transparentní a flexibilní. Vyšší míra flexibility je také výhodná pro vyjednávání s jednotlivými dodavateli o ekonomických a technických podmínkách.

P05: Nákup a vývoj

- U nákupu standardizovaných komerčních produktů je požadována schopnost nastavení balíkového řešení interními kapacitami či nezávislými externími dodavateli.
- U standardizovaných agend je preferován nákup a úprava před zakázkovým vývojem nového zákaznického řešení.
- Vzájemné integrace musí být realizované přes aplikační middleware. Integrovaní scénáře zajišťují, aby implementace nových funkcí v řídicí aplikaci minimalizovala vyvolané změny na straně návazných aplikací.
- Preferujeme přírůstkovou integraci před přenosem kompletních informací.
- Preferujeme řešení v min. třívrstvé či vícevrstvé architektuře s min. oddělením databázové, aplikační a prezentační vrstvy.
- Minimalizujeme dodávku řešení s takovými úpravami, které by omezovaly nebo eliminovaly přechod na budoucí vyšší verze produktu.
- V transakčních systémech preferujeme pouze základní operativní reporting. Plný reporting je implementovaný v analytických nástrojích.
- Řešení je řádně dokumentované po stránce vývojové, provozní a uživatelské.
- Případné zdrojové kódy jsou verzovány a ověřeny, že z nich je možno vytvořit interními týmy Správy železnic build aplikace. Zdrojové kódy a dokumentace jsou ukládány na standardizované úložiště Správy železnic.
- Návrh prostředí reflektuje trendy technologií a zároveň business potřeby.

Zdůvodnění: Regulace nákupu a do-vývoje integrací a aplikací slouží k co nejsrozumitelnějšímu a transparentnímu užívání daných technologií. Díky danému postupu v nákupu a vývoji je možné se efektivně vyrovnat s novinkami, které nově nakoupené produkty představují.

P06: Business kontinuita jako zásadní činnost

- Navržené řešení musí odpovídat kritičnosti aplikace a požadovaným parametrům SLA.
- Servisní model a parametry aplikace odpovídají bezpečnostní klasifikaci a byznysové kritičnosti aplikace.
- Dle servisního modelu jsou definované plány obnovy a „disaster recovery“ postupy.

Zdůvodnění: Správa železnic jakožto správce železniční dopravní cesty, kritické infrastruktury státu, musí být připraven na případné narušení provozu, a proto musí požadovat taková řešení, která umožní zajistit kontinuitu a obnovu klíčových procesů, činností a systémů organizace.

5 Služby Platformy SŽ

Tato kapitola popisuje seznam komoditních ICT služeb a jednotlivých HW/SW komponent, které tvoří standard v rámci Správy železnic. Cílem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím ICT prostředím a v maximální míře využít již provozované komponenty a technologie. Seznam služeb a komponent je průběžně aktualizován.

ICT služby Platformy jsou rozděleny do následujících skupin (kategorií):

- **Infrastrukturní**
Infrastrukturní službou je míněno poskytování IT infrastruktury na úrovni HW, virtualizace, operačních systémů a diskových úložišť.
- **Platformní**
Platformní služba poskytuje databázovou platformu či portálové řešení, které integruje webové aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační protokoly a formáty dat.
- **Podpůrné**
Podpůrné služby zajišťují komplexní správu a provoz IT infrastruktury. Například monitorovací systémy, zálohování, reporting. Podpůrné služby jsou povinné k využití dodavatelem, pokud není jinak určeno SŽ.

5.1 Infrastrukturní služby

5.1.1 Služba virtuálních strojů

Služba virtuálních strojů (dále jen „VM“) je provozována na vysoce dostupné virtualizační technologii VMware a hardware s procesory Intel Xeon E5-26XX, Intel Silver 4215. Všechna VM s operačním systémem Windows Server mají nainstalován balík VMware Open Tool.

Parametry služby jako sizing virtuálních strojů, výběr OS podporovaných Platformou SŽ 2.0, počet a konfigurace síťových karet jsou konfigurovány individuálně na základě požadavků projektu, resp. dodávaného řešení.

SŽ zajišťuje vysokou dostupnost služby virtuálních strojů na úrovni vi, a to v rámci jednoho datového centra. Pokud služby dodávaného řešení vyžadují zajištění vysoké dostupnosti, tato musí být zajištěna dodavatelem v rámci dodávky včetně služby loadbalancingu.

Služba	Popis
Win.VMware.x86_64	Služby virtuálního serveru s operačním systémem Windows Server na virtualizaci VMware a architektuře x86_64
RHEL.VMware.x86_64	Služby virtuálního serveru s operačním systémem RHEL (RedHat Enterprise Linux) na virtualizaci VMware a architektuře x86_64
SLES.VMware.x86_64	Služby virtuálního serveru s operačním systémem SLES (SUSE Linux Enterprise Server) na virtualizaci VMware a architektuře x86_64 Omezení: Využití pro výhradně pro SAP

5.1.2 Služba datového úložiště

Služba datového úložiště je provozována na datových úložištích typu SAN, která jsou osazena 10K SAS disky v RAID5 (+hotspare disk) případně RAID 6, nebo disky SSD v RAID5 (+hotspare disk) pro aplikace vyžadující vyšší výkon, typicky databáze. V rámci služby datového úložiště není poskytována služba replikace mezi SAN úložišti, ani služba tieringu. V primárním datovém centru CDP je dále provozováno škálovatelné, výkonné, softwarově-definované datové úložiště postavené na technologii VMware vSAN, využívající prostředků fyzických serverů x86 a jejich komponent (cpu, ram, nic a disk). VMware vSAN je nativně integrované s hypervisorem VMware ESXi.

Služba	Popis
Lokální datový disk 10K	Služba datového úložiště, provozovaného na SAN storage a 10K discích v RAID 5 (+hotspare) případně RAID 6 poli, pro systémové a datové disky.
Lokální datový disk SSD	Služba datového úložiště, provozovaného na SAN storage osazeného SSD disky v poli RAID5 (+hotspare).

5.2 Platformní služby

Platformní služba (PaaS – Platform as a Service) poskytuje databázovou či integrační platformu (middleware). Tato integruje aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační protokoly a formáty dat.

V rámci platformy Správy železnic jsou poskytovány tyto platformní služby:

5.2.1 Služba zabezpečeného portálového řešení

Služba	Popis
Liferay na Win.VMware.x86_64	Liferay je přední open-source podnikové portálové řešení založené na jazyce Java, které umožňuje správu dat, aplikací, procesů a integrace současných i nových aplikací z jednoho centrálního uživatelského rozhraní.

5.2.2 Služby zabezpečených webových serverů

Služba	Popis
Microsoft IIS na Win.VMware.x86_64	Služba webového serveru postavená na technologii Microsoft Internet Information Services (IIS) provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.
Apache HTTP Server na Win.VMware.x86_64	Služba webového serveru postavená na open-source technologii Apache provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.
Apache HTTP Server na RHEL.VMware.x86_64	Služba webového serveru postavená na open-source technologii Apache provozovaná na serverech s operačním systémem RHEL s virtualizací VMware.

5.2.3 Služby zabezpečených aplikačních serverů

Služba	Popis
.NET na Win.VMware.x86_64	Aplikační server Microsoft .NET prostředí pro vývoj a provoz aplikací založených na .NET frameworku
JBOSS na Win.VMware.x86_64	Služba virtuálního aplikačního serveru JBOSS provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.
Oracle WebLogic na RHEL.VMware.x86_64	Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem RHEL s virtualizací VMware.
Oracle WebLogic na SLES.VMware.x86_64	Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem SLES s virtualizací VMware.
Oracle WebLogic na Win.VMware.x86_64	Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem Windows Server s virtualizací VMware.

5.2.4 Služby zabezpečených databázových prostředí

Služba	Popis
Oracle DB na Oracle Exadata	Databázová služba Oracle DB provozovaná na optimalizovaném hardware Oracle Exadata Database Machine – kombinovaná hardwarová a softwarová platforma.
MS SQL na Win.VMware.x86_64	Služba virtuálních databázových serverů MS SQL Server provozovaná na serverech s operačním systémem Windows Server a virtualizační platformě VMware.

5.3 Podpůrné služby

Podpůrné služby standardně poskytované k využití pro dodávaná ICT řešení.

5.3.1 Bezpečnost

Služby zabezpečení infrastruktury.

Služba	Popis
Antivirus	Antivirové řešení fSecure, provozované jako virtuální appliance, zajišťuje ochranu koncových stanic a serverové infrastruktury před škodlivým obsahem, zejména malwarem, exploity, síťovými útoky a jinými bezpečnostními hrozbami. Každé datové centrum Správy železnic disponuje vlastní virtuální appliance fSecure. Nasazením antivirového řešení fSecure jako virtuální appliance, jsou minimalizovány konzumované výpočetní zdroje a dopad na výkon virtualizační infrastruktury.
PAM	Privileged Access Management (PAM) je řešení které pomáhá kontrolovat, monitorovat, zabezpečit a auditovat privilegované identity před jejich zneužitím. Omezení: Aktuálně v pilotním provozu
IDM	Identity Management (IDM) je řešení umožňující řízení uživatelských účtů a jejich oprávnění napříč systémy. IDM umožňuje lepší přehlednost, bezpečnost a automatizaci. V prostředí Správy železnic bylo implementováno open-source řešení MidPoint společnosti Evolveum, jenž nevyžaduje nákup licencí. Toto řešení má otevřenou a rozšiřitelnou architekturu založenou na standardech Java, XML a REST.
Active Directory and Domain Services	Adresářová služba společnosti Microsoft pro správu zařízení a identit a jejich autentizaci a autorizaci v podnikových sítích. Dodávaná řešení musí podporovat integraci na službu Active Directory Správy železnic. Správa železnic provozuje multi-forest prostředí, proto musí aplikace umožňovat využití více AD konektorů, za účelem ověření uživatelů.

5.3.2 Monitoring, alerting

Služba	Popis
Monitoring	
Zabbix	Služba dohledu infrastruktury je zajištěna pomocí dohledových agentů instalovaných na provozovaném prostředí nebo bez-agentově se vzdáleným dohledem, sledování standardními protokoly SNMP, HTTP, HTTPS apod. Dodavatelé ve spolupráci s jednotkou SŽT zajistí napojení dodávaných řešení na monitoring Zadavatele. Tím není dotčena případná povinnost dodavatele řešení monitorovat kvalitu a dostupnost dodávaného řešení v rámci vlastního monitoringu.

5.3.3 Aktualizace systémů, Distribuce aplikací

Služba	Popis
Aktualizace	
Distribuce SW a aktualizace koncových stanic	Technologií System Center Configuration Manager (SCCM) je zajištěna distribuce softwarových balíčků a aktualizace koncových stanic. Patchování klientských stanic probíhá 1 x měsíčně a je plně v gesci Správy železnic.
Aktualizace serverových operačních systémů	Aktualizace serverových operačních systému Windows Server je řešena skriptovacím jazykem Powershell. Patchování serverových operačních systémů probíhá 1 x měsíčně a je zajištěno Správou železnic, pokud není s dodavatelem řešení dohodnuto jinak. Aktualizace serverových operačních systémů založených na linuxové distribuci je prováděna manuálně, na vyžádání správce aplikace, nebo v reakci na kybernetické hrozby.

5.3.4 Zálohování

Služba	Popis
Zálohování a obnova	Služba zálohování prostředí je zajištěna technologií IBM Spectrum Protect (TSM – Tivoli Storage Manager) komplexním řešením pro fyzické fileservery, virtualizované prostředí a širokou škálu aplikací. IBM Spectrum Protect zálohuje data s využitím technologie VMware snapshot. Služba zálohování umožňuje 3 základní typy zálohování: Snapshot disku pro dosažení rychlé obnovy celého OS v Crash Consistent stavu včetně aplikační konfigurace. Zpravidla je takto zálohován pouze systémový oddíl

Služba	Popis
	<p>virtualizovaného serveru. Záloha probíhá jednou denně a retence je nastavena na 30 posledních verzí.</p> <p>Záloha datových svazků připojených k jednotlivým serverům, pro dosažení max. možné odolnosti proti náhodnému smazání či poškození apod. Záloha probíhá jednou denně, kdy se uchovává 90 posledních verzí souborů a poslední smazaná verze souboru je uchovávána 365 dní.</p> <p>Zálohy Oracle nebo SQL databází pomocí agentů. Záloha probíhá dvakrát denně. Přes den jsou zálohovány transakční logy databází, v noci pak vlastní databáze. Retence je nastavena na 60 posledních verzí.</p>

5.3.5 Komunikační infrastruktura

Služba	Popis
DNS	Domain Name System (DNS) je kritickou službou, která má zásadní vliv na bezpečnost, odezvu a dostupnost služeb SŽ. Je nezbytná pro správný chod podnikové sítě a služeb na bázi Active directory. Správa železnic provozuje interní i externí službu DNS.
Firewall	Firewall soustava je velmi důležitým uzlem veškeré komunikace v síti SŽ, jenž pomocí pravidel filtruje síťový provoz a chrání prostředky v síti Správy železnic.
Proxy	Proxy soustava zajišťuje přístup uživatelů a serverů k internetu. Naprostá většina komunikace uživatelů do internetu prochází přes ni, jiný přístup není povolen. Proxy servery fungují jako prostředník mezi klienty a cílovými servery, mimo perimetr sítě SŽ, překládá klientské požadavky a vůči cílovému serveru vystupuje sám jako klient.
Reverzní proxy	Všechna připojení z internetu směřující na některý ze serverů jsou směrována přes reverzní proxy server, který buďto požadavek zpracuje sám nebo ho předá dál serverům. Umožňuje SSL terminaci a kompresi.
VPN	Služba virtuální privátní sítě, umožňující dodavateli zabezpečený přístup k prostředkům datových center Správy železnic.
VPN S2S	Služba virtuální privátní sítě Site-to-Site.

6 Technologie Platformy SŽ

Tato kapitola popisuje technologie, jež tvoří základ k výše uvedeným infrastrukturním a platformním službám.

Tyto softwarové a hardwarové prostředky nesmějí být přímo použity v návrhu řešení. Jejich použití je možné pouze prostřednictvím výše uvedených infrastrukturních nebo platformních služeb.

Pro některé případy výběrových řízení pro aplikační software je přípustné použití tzv. zapouzdřených technologií, jež nejsou součástí Platformy SŽ, ale nabízené řešení vyžaduje jejich nasazení.

Zapouzdřená technologie je zpravidla součástí jiné primární technologie jako tzv. podpůrný program. Takový program nevyžaduje samostatnou instalaci, jelikož je instalován jako součást dané komponenty.

Použití takových zapouzdřených technologií je možné jen v následujících případech:

1. Jejich použití nebude klást žádné dodatečné provozní, finanční ani implementační nároky po celou dobu životnosti primární technologie.
2. Nebudou vyžadovat žádné dodatečné licence nad rámec licencí hlavního dodávaného řešení.
3. Aktualizace zapouzdřených technologií bude probíhat pouze současně s aktualizací hlavního dodávaného řešení.
4. Jejich podpora bude poskytována současně a ve stejném rozsahu jako podpora hlavního dodávaného řešení.
5. Zapouzdřené technologie nebudou vyžadovat žádné speciální provozní či bezpečnostní zajištění.

Při použití zapouzdřených technologií je nutné danou technologii identifikovat nejméně v následujícím rozsahu:

- Název
- Verze
- Výrobce
- Licence
- Termín a úroveň podpory

Technologie	Popis
Integrace	
LifeRay	Bezplatný open-source podnikový portál založený na jazyce Java, umožňující správu dat, aplikací a procesů.
Aplikační servery	
Microsoft Internet Information Services (IIS)	Framework pro běh třívrstevných podnikových aplikací s kolekcí rozšiřujících modulů provozovaný nad operačními systémy Windows, vytvořený společností Microsoft.
Oracle WebLogic Server	Aplikační server Oracle WebLogic Server (WLS) pro provoz aplikací na platformě J2EE
JBoss	Aplikační server JBoss pro provoz platformy J2EE pro řešení s potřebou autonomního prostředí, nebo pro aplikace nepožadující vysokou dostupnost
Webové servery	
Apache HTTP Server	Webový server postavený na open-source technologii Apache.
MS IIS	Webový server s kolekcí rozšiřujících modulů provozovaný nad operačními systémy Windows, vytvořený společností Microsoft.
Databázové systémy	
Oracle Database	Relační databázový systém společnosti Oracle určený pro mission critical aplikace.
Microsoft SQL	Relační a analytický databázový systém Microsoft SQL Server.
Serverové operační systémy	
Windows Server	Operační systém, na němž jsou provozovány aplikační či webové služby a databázové stroje založené zejména na technologiích společnosti Microsoft.
RHEL	Operační systém RedHat Enterprise Linux (RHEL) je linuxová distribuce společnosti RedHat určená pro komerční sféru. Použití pro aplikační servery.
SLES	Operační systém SUSE Linux Enterprise Server (SLES) je linuxová distribuce společnosti SUSE určená pro komerční sféru. Použití pro aplikační servery.
Virtualizační platformy	
VMware	Primární virtualizační platforma pro virtualizaci hardwarové platformy x86_64. Tato zajišťuje business kontinuitu, škálovatelnost a flexibilitu provozu pro operační systémy. Platforma je primárně určena pro virtualizaci operačních systému Windows, případně Linux.
Oracle VM	Virtualizační platforma Oracle, pro virtualizaci hardwarové platformy x86_64 založena na technologii Citrix Xen Hypervisor. Omezené využití: Primárně určena pro provoz Oracle DB.
Hardware	
x86_64	Servery postavené na architektuře x86_64 – 64bitové procesory, provozovány na platformě Intel 2-socketových serverech typu rack a blade.
SAN datová uložení	Uložení dat s podporou vysoké dostupnosti, škálování a vysokou úrovní zabezpečení. Podporuje vytváření snapshotů, replikaci dat a automatický tiering datových uložení.
Network and Security	
VPN	Zabezpečený vzdálený přístup do sítě SŽ je řešen pomocí technologie Cisco ASA.
Firewall	Zabezpečení pomocí firewall pravidel je zabezpečeno technologií Cisco.

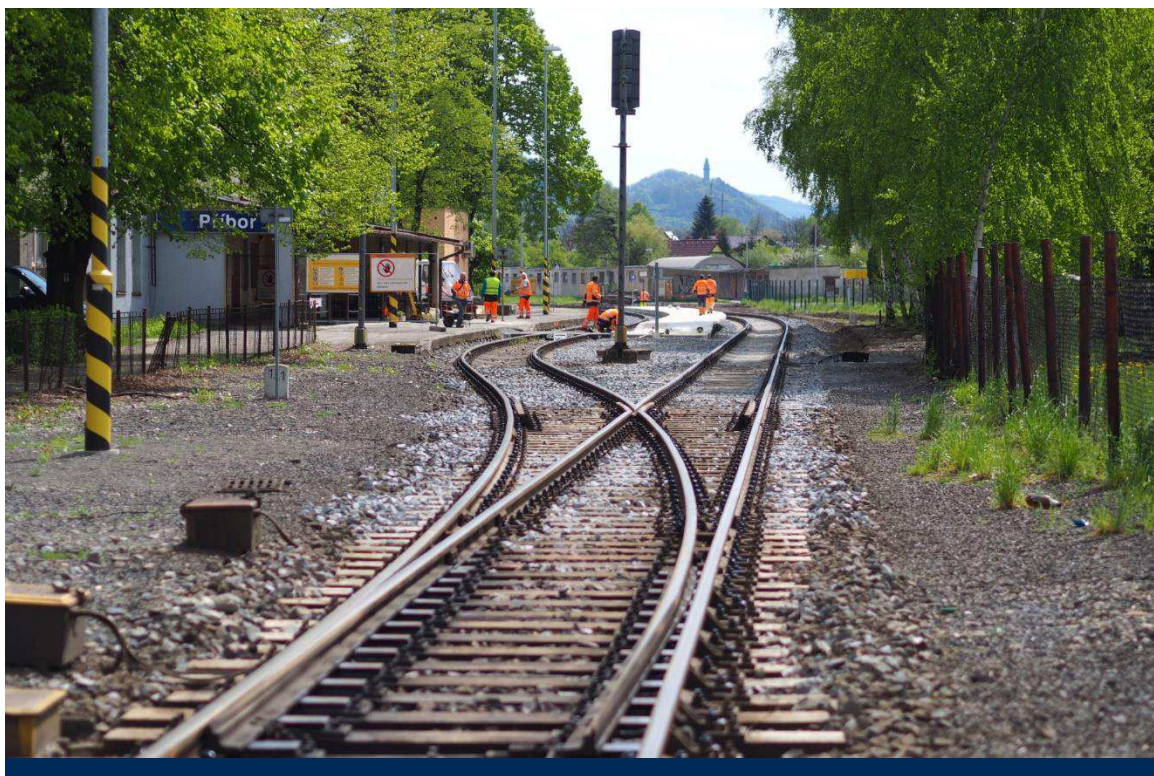
7 Přílohy

Příloha 1 – Standardy vývoje informačních systémů Správy železnic

Správa železnic, státní organizace
Název organizační jednotky
Dlážděná 1003/7
110 00 Praha 1

© 2022

Datum tisku
2022-04-2931



Standardy vývoje informačních systémů Správy železnic

Březen 2022

Historie verzí

Verze	Popis	Platnost od	Předchozí verze
0.1	Draft	22. 3. 2022	
1.0	První verze dokumentu	31. 3. 2022	

Obsah

Seznam zkratk a pojmů.....	3
1 Standardy vývoje informačních systémů Správy železnic	4
1.1 Dvouvrstvá architektura	4
1.1.1 Datová vrstva.....	4
1.1.2 Aplikační vrstva	4
1.2 Třívrstvá a vícevrstvá architektura	4
1.2.1 Datová vrstva.....	5
1.2.2 Aplikační vrstva	5
1.2.3 Prezentační vrstva	5
1.2.4 Integrovaná vrstva	5
1.3 Požadavky na prezentační vrstvu	6
1.3.1 Uživatelské rozhraní (User Interface, UI)	6
1.3.2 Uživatelský prožitek (User Experience, UX)	6
1.4 Bezpečnost	7
1.4.1 Zabezpečení aplikací	7
1.4.2 Autentizace a autorizace	8
1.4.3 GDPR	8
1.5 Dokumentace	8
1.5.1 Technická dokumentace jádra systému.....	8
1.5.2 E-R modely databáze	8
1.5.3 Objektový model pro aplikace	8
1.5.4 Procesní diagramy, schémata toků dat	8
1.5.5 Komunikační rozhraní.....	8
1.5.6 Drátové modely všech obrazovek uživatelského rozhraní aplikací.....	9
1.5.7 Popis konfigurace provozního prostředí.....	9
1.5.8 Uživatelská příručka	9
1.5.9 Příručka administrátora	9
1.6 Předávání vývoje do provozu	9

Seznam zkratk a pojmů

3NF	Třetí normální forma
API	<i>z angl. Application Programming Interface</i> , rozhraní pro programování aplikací
APP	Aplikační vrstva
AS	Aplikační server
DB	Databáze
DBMS	<i>z angl. Database Management System</i> , Systém řízení databáze
DC	Datové centrum
DDL	<i>z angl. Data Definition Language</i>
DR	<i>z angl. Disaster Recovery</i> , Obnova po havárii
HA	<i>z angl. High Availability</i> , Vysoká dostupnost
HW	Hardware označuje veškeré fyzicky existující technické vybavení počítače
JSON	<i>z angl. JavaScript Object Notation</i> , JavaScriptový objektový zápis
OS	Operační systém
SQL	Structured Query Language, standardizovaný dotazovací jazyk pro práci v relačních databázích
SW	Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost
SŽ	Správa železnic, státní organizace
WS	Webový server
XML	<i>z angl. Extensible Markup Language</i> , obecný značkovací jazyk

1 Standardy vývoje informačních systémů

Správy železnic

Při vývoji software ve Správě železnic je požadováno, aby byly plně respektovány obvyklé metodiky a best-practice pro návrh a vývoj software pomocí vícevrstvé architektury. Konkrétní užití jednotlivých vzorů se řídí vhodností, plánovanou zátěží a požadavky na dostupnost vyvíjeného software.

1.1 Dvouvrstvá architektura

Dvouvrstvou architekturu při vývoji software lze využít v případě, kdy se jedná o menší, samostatný software, který nebude integrován na další informační systémy, nebo datové zdroje Správy železnic. Užití takového software je plánováno pro menší desítky uživatelů, bez požadavku na vysokou dostupnost a možnosti škálování výkonu a rozložení zátěže prostřednictvím clusterování. U tohoto typu software nejsou definovány požadavky na vysokou odolnost proti chybám, rychlou reakci systému, nebo správu dat pro velké sítě.

Využití dvouvrstvé architektury musí být předem diskutováno s Oddělením IT architektury, které v odůvodněných případech vydá příslušnou výjimku.

1.1.1 Datová vrstva

Realizace datové vrstvy je požadována prostřednictvím preferované relační databáze (dle služeb Platformy) a respektováním metodiky 3NF. Je požadován jednoznačný datový model s minimální redundancí dat a datové struktury budou modelovány a popsány jazykovými konstrukcemi DDL, které jsou kompatibilní s určeným databázovým systémem.

Celá struktura dat bude popsána formálně prostředky E-R modelování. K datovému modelu je požadováno dodat korespondující SQL DDL skripty, který budou plně odpovídat dodané databázi. Je požadováno, aby správnost, úplnost a optimalizace datového modelu byla řešena již v rámci návrhu řešení.

V rámci dvouvrstvé architektury je umožněno, aby logika byla rozprostřena částečně v databázi a částečně v aplikační, resp. prezentační vrstvě.

1.1.2 Aplikační vrstva

Aplikační vrstva a prezentační vrstva je ve dvouvrstvé architektuře realizována jako jedna, společná a nedělitelná vrstva. Je požadováno, aby tato vrstva byla realizována v souladu s principy objektově orientovaného programování a komunikace mezi vrstvami byla realizována standardními zabezpečenými a šifrovanými protokoly. Je požadováno, aby uživatelské identity nebyly z aplikační vrstvy prezentovány do datové vrstvy, přičemž tyto vrstvy musí mezi sebou komunikovat technickým účtem, k tomu účelu v databázi vytvořeném.

Je požadováno, aby aplikační vrstva podporovala Multitasking, tedy umožňovala provádění několika procesů současně a systém byl již v rámci návrhu a vývoje optimalizován plánovaný výkon.

V rámci vývoje musí být ošetřena všechna bezpečnostní rizika popsaná v kapitole 1.4.

1.2 Třívrstvá a vícevrstvá architektura

Třívrstvá a vícevrstvá architektura je požadována při vývoji software ve všech případech mimo výjimky definované v kap. 1.1. Specifikace řešení vyžadující třívrstvou architekturu tak může disponovat následujícími vlastnostmi:

- Má být integrován na jiný software Správy železnic, nebo software třetích stran, a to z důvodu jednotného přístupu k datům a procesům vyvíjeného software
- Je plánováno využití pro větší počty uživatelů
- Je požadována vysoká dostupnost (HA)

- Je požadován Clustering pro rozložení zátěže a škálování výkonu
- Je požadována vysoká odolnost proti chybám, rychlá reakce systému, nebo správa dat pro velké sítě

1.2.1 Datová vrstva

Realizace datové vrstvy je požadována prostřednictvím preferované relační databáze (dle služeb Platformy) a respektováním metodiky 3NF. Je požadován jednoznačný datový model s minimální redundancí dat, datové struktury budou modelovány a popsány jazykovými konstrukcemi DDL, které jsou kompatibilní s určeným databázovým systémem.

Celá struktura dat bude popsána formálně prostředky E-R modelování. K datovému modelu je požadováno dodat korespondující SQL DDL skripty, který budou plně odpovídat dodané databázi. Je požadováno, aby správnost, úplnost a optimalizace datového modelu byla řešena již v rámci návrhu řešení.

V rámci třívrstvé a vícevrstvé architektury není umožněno, aby logika byla rozprostřena částečně v databázi a částečně v aplikační vrstvě. Aplikační logika je tak striktně pouze v aplikační vrstvě.

1.2.2 Aplikační vrstva

Je požadováno, aby tato vrstva byla realizována v souladu s principy objektově orientovaného programování a komunikace mezi vrstvami byla realizována standardními zabezpečenými a šifrovanými protokoly. Je požadováno, aby uživatelské identity nebyly z aplikační vrstvy prezentovány do datové vrstvy, přičemž tyto dvě vrstvy musí mezi sebou komunikovat technickým účtem, k tomu účelu v databázi vytvořeném.

Je požadováno, aby aplikační vrstva podporovala Multitasking, tedy umožňovala provádění několika procesů současně a v již rámci návrhu a vývoje optimalizovat plánovaný výkon.

V rámci vývoje musí být ošetřena všechna bezpečnostní rizika popsaná v kapitole 1.4.

1.2.3 Prezentační vrstva

Pro interakci s uživatelem je požadováno, aby prezentační vrstva byla realizována desktopovým klientem (tlustým), nebo webovým klientem (tenkým), a to v závislosti na vhodnosti použití a požadavcích na software kladených. Komunikace mezi prezentační a aplikační vrstvou musí být realizována standardními zabezpečenými a šifrovanými protokoly.

V rámci prezentační vrstvy a desktopového klienta je možné přenesením části aplikační logiky na klienta, tedy využití prostředků klientské stanice ke zvýšení výkonu systému, ale pouze za předpokladu, že tento systém bude zabezpečovat konzistenci aplikační logiky, napříč všemi desktopovými klienty.

Bez aktualizčních mechanismů, které zajistí stejné verze software, na všech klientských stanicích v reálném čase není tato možnost povolena.

1.2.4 Integrační vrstva

V případě, kdy vyvíjený software má být integrován na jiný software Správy železnic, nebo software třetích stran, je požadováno, aby tato integrační vrstva byla realizována jako samostatná vrstva, umožňující škálování výkonu a rozložení zátěže.

Realizace integrací mezi aplikačními komponentami musí splňovat principy SOA. Veškerá komunikace tedy musí probíhat prostřednictvím definovaných služeb rozhraní, a není tedy povolena výměna dat prostřednictvím přímých vazeb, jako je sdílení paměti, souborů, nebo databází. Pokud je k dispozici, komunikace probíhá prostřednictvím k tomu určené sběrnice (ESB) nebo integrační platformy.

V případě, že má být vyvíjena komponenta integrována se **spisovou službou SŽ**, musí splňovat požadavky na integraci prostřednictvím Národního standardu pro elektronické systémy spisové služby¹ a integrace musí být rozhraními definovanými v tomto standardu také realizována.

V případě, že má být vyvíjena aplikace integrována s programovým prostředím komponent **systému SAP**, musí být realizována prostřednictvím určené integrační platformy (SAP Cloud Platform, příp. produktu, která jej nahradí). Detailní parametry požadavku na integraci budou definovány v příslušných případech.

1.3 Požadavky na prezentační vrstvu

1.3.1 Uživatelské rozhraní (User Interface, UI)

Pomocí uživatelského rozhraní může uživatel komunikovat se zařízením, počítačem a programy. Při navrhování vysoce kvalitního uživatelského rozhraní je požadováno zohlednit nejen vzhled rozhraní, ale také jeho logickou strukturu, aby s ním uživatel mohl snadno a rychle komunikovat a dosáhnout požadovaného výsledku bez zbytečného úsilí. Cílem je vytvořit rozhraní, které poskytuje jednoduchou, srozumitelnou a pohodlnou interakci uživatele s informačním systémem.

Pro návrh UI informačních systémů SŽ platí následující zásady:

- standardní ovládací prvky
- uživatelské rozhraní jednoduché a přehledné
- konzistentní prostředí
- účelné rozvržení obrazovek
- barvy a písma dle grafického manuálu
- hierarchie daná typograficky
- informování uživatele, co systém právě dělá
- odpovídající tvar a velikost ovládacích prvků
- kódování znaků UNICODE
- datumové položky dle českého standardu „DD.MM.RRRR“
- jednotný vizuální styl (pro některé projekty dle korporátní identity)
- responzivní design webových aplikací

1.3.2 Uživatelský prožitek (User Experience, UX)

UX je to, co uživatel pocítí a pamatuje si v důsledku použití aplikace, systému nebo webu. UX musí být bráno v úvahu při vývoji uživatelského rozhraní, vytváření informační architektury a testování použitelnosti informačních systémů SŽ. Po určení cílového publika a charakteristiky uživatelů je požadováno vytvořit seznam UX požadavků na projekt.

UX informačních systémů SŽ musí mít následující vlastnosti:

- cílem je efektivní uživatel
- návodné ovládání
- ergonomie
- jednoduché, intuitivní
- pravidla přístupnosti, tam kde je požadováno
- zobrazování relativních a požadovaných dat
- rychlost odezvy (doba zpracování požadavku od uživatele by na serveru neměla přesáhnout 0,5s, tak aby celková doba odezvy uživatelský ovládacích prvků byla kratší než 0,8s. V případě, že je předpokládán čas odezvy delší než 0,8s, ale kratší než 2s

¹ NSESSS, <https://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx>

- bude uživateli zobrazen wait cursor a pokud bude předpokládán čas odezvy delší než 2s bude pro informaci uživatele použit progress bar zobrazující průběh operace.)
- použití lazy loading v odůvodněných případech
- jednotná terminologie v celém systému
- ne všechno na jedné obrazovce
- ne všechno v rozbalovacím menu (příliš mnoho položek)
- navigace, kde se uživatel v aplikaci nachází
- minimalizace použití dlouhých textů
- vhodné využití grafických a obrazových prvků
- nepoužívat drobný text
- pečlivé plánování dialogů (logické skupiny)
- ne překrývající se dialogy
- jednotné, stejné ovládací prvky v dialozích na stejných místech s popisky s jednotnou terminologií

1.4 Bezpečnost

Všechny vyvíjené aplikace musejí splňovat požadavky kladené platnou legislativou a interními předpisy Správy železnic.

Klíčovým dokumentem z pohledu požadavků na vyvíjený software je „Provozní politika prvků v působnosti systému řízení bezpečnosti informací“, který specifikuje požadavky pro následující oblasti:

- Zálohování a obnova
- Bezpečnost komunikací
- Řízení přístupu
- Ochrana před škodlivým kódem
- Logování a monitoring
- Bezpečné předávání a výměna informací
- Akvizice, vývoj a údržba

1.4.1 Zabezpečení aplikací

Je požadováno, aby jednotlivé vrstvy splňovaly minimálně tyto požadavky:

- Ke komunikaci mezi jednotlivými vrstvami je používán systémový účet, který lze v případě ohrožení kybernetické bezpečnosti deaktivovat, nebo změnit.
- Systémový účet, který je využíván ke komunikaci mezi vrstvami není privilegovaným účtem.
- Všechny vrstvy jsou ošetřeny proti nejzávažnějším bezpečnostním rizikům jako jsou²:
 - Injection
 - Broken Authentication
 - Sensitive Data Exposure
 - XML External Entities (XXE)
 - Broken Access Control
 - Security Misconfiguration
 - Cross-Site Scripting (XSS)
 - Insecure Deserialization
 - Using Components with Known Vulnerabilities
 - Insufficient Logging&Monitoring
- Jednotlivé vrstvy uchovávají své konfigurační parametry v šifrované podobě.

² Dle aktuálního seznamu nejzávažnějších bezpečnostních rizik definovaných OWASP (<https://owasp.org/>).

1.4.2 Autentizace a autorizace

1.4.2.1 Autentizace

Autentizace je proces ověření proklamované identity subjektu. Je požadováno, aby aplikace umožňovala následující typy autentizace:

- SSO (Single Sign-On), autentizaci pomocí protokolu Kerberos, nebo OpenID proti Active Directory
- Manuální přihlášení, autentizaci pomocí vyvíjeného software, tzn. Uživatelská jména a hesla jsou uložena v databázi v šifrované podobě.
- Autentizaci pomocí protokolu LDAP, proti Active Directory
- 2FA

1.4.2.2 Autorizace

Je požadováno, aby vyvíjený software obsahoval vlastní autorizační modul, který bude minimálně umožňovat:

- Vytváření uživatelských účtů
- Vytváření rolí
- Přidělování jednotlivých uživatelských účtů k rolím
- Přidělování konkrétních oprávnění na role

V rámci naplnění povinností vyplývajících ze zákona č. 181/2014 Sb. a vyhlášky č. 82/2018 Sb. je požadováno, aby vyvíjený software umožňoval správu uživatelů a rolí pomocí externího nástroje na řízení identit, tj. Identity managementem implementovaným ve Správě železnic. Integrace mezi vyvíjeným softwarem a Identity management bude realizována prostřednictvím integrační vrstvy vyvíjeného software.

1.4.3 GDPR

Je požadováno kompletní splnění všech požadavků na zpracování osobních údajů dle zákona č. 110/2019 Sb. Analýza a návrh opatření musí být řešen již v rámci návrhu řešení.

1.5 Dokumentace

Je požadováno, aby součástí dodávky vyvíjeného software byla dokumentace, a to minimálně v rozsahu:

1.5.1 Technická dokumentace jádra systému

Dokumentace jádra systému, jeho funkcí, služeb a rozhraní. Dokumentace bude obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.

1.5.2 E-R modely databáze

Kompletní dokumentace ve formě E-R schémat pro všechny implementované databáze včetně korespondujících DDL SQL skriptů.

1.5.3 Objektový model pro aplikace

Dokumentace obsahující objektové modely všech funkcí, jejich komponent, modulů, vztahů.

1.5.4 Procesní diagramy, schémata toků dat

Dokumentace obsahující procesní diagramy a mapu všech toků dat celého řešení.

1.5.5 Komunikační rozhraní

Dokumentace všech typů komunikačních rozhraní, všech jejich registrovaných služeb a všech funkcí, struktur dat a vlastností těchto služeb.

1.5.6 Drátové modely všech obrazovek uživatelského rozhraní aplikací

Dokumentace všech částí software musí obsahovat drátové modely všech obrazovek uživatelského rozhraní včetně popisu funkcí prvků každé obrazovky.

1.5.7 Popis konfigurace provozního prostředí

Dokumentace musí obsahovat soupis všech požadavků na nastavení hardwarových a softwarových komponent běhového prostředí jako jsou:

- mapování souborových systémů
- požadavky na operační paměť a počty jader
- konfigurační parametry jednotlivých podpůrných SW prostředků (např. specifika pro nastavení databáze, aplikačního serveru, webového serveru, apod.)

1.5.8 Uživatelská příručka

Příručka bude distribuována uživatelům. Musí obsahovat kompletní popis všech uživatelských funkcí pro práci se software. Příručka bude využívána jako základní materiál pro školení nových uživatelů. Příručka musí obsahovat kvalitně a jednoznačně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek. Musí být napsána v českém jazyce a před finálním odevzdáním zpracovaná jazykovým korektorem.

1.5.9 Příručka administrátora

Příručka bude distribuována úzké skupině uživatelů, administrátorům systému. Musí obsahovat kompletní popis všech funkcí pro práci s administrací software. Příručka bude využívána jako materiál pro školení nových administrátorů. Příručka musí obsahovat kvalitně a jednoznačně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek. Musí být napsána v českém jazyce a před finálním odevzdáním zpracovaná jazykovým korektorem.

1.6 Předávání vývoje do provozu

Pokud nebude určeno jinak, veškeré výstupy (zdrojové kódy, konfigurační soubory, testovací data, dokumentace atp.) musejí být předávány prostřednictvím určeného repositáře.

Příloha č. 5 zadávací dokumentace

HARMONOGRAM PLNĚNÍ

Etapa	Popis	Odkaz na kapitulu v TS	Termín zahájení	Požadovaný termín dokončení
Etapa 1A	<ul style="list-style-type: none"> Před-implementační analýza 	4.1.1	Od účinnosti smlouvy	1 měsíc
Etapa 1B	<ul style="list-style-type: none"> Instalace komponent LM Napojení určených zdrojů logů (z vybraných lokalit) Dodávka produktových licencí včetně podpory výrobce v délce 60 měsíců 	4.1.2 4.1.3	Od ukončení Etapy 1A, nebo od připravenosti Platformy SŽ	3 měsíce
Etapa 2	<ul style="list-style-type: none"> Napojení všech určených zdrojů logů pro etapu 2 	4.1.3	Od ukončení Etapy 1B	8 měsíců
Etapa 3	<ul style="list-style-type: none"> Tvorba a optimalizace bezpečnostní / detekční politiky řešení Školení 	4.1.4 4.1.5	Od ukončení Etapy 1B	8 měsíců
Etapa 4	<ul style="list-style-type: none"> Napojení určených zdrojů logů pro etapu 4 	4.1.3	Od ukončení Etapy 2	4 měsíce
Etapa 5	<ul style="list-style-type: none"> Technická podpora servisního týmu SŽ Údržba řešení 	4.2.1 4.2.2	Od ukončení Etapy 1B	60 měsíců
Etapa 6	<ul style="list-style-type: none"> Konzultace a rozvojové aktivity 	4.2.3	Od účinnosti smlouvy	Do konce účinnosti smlouvy

Příloha č. 6 zadávací dokumentace

Smlouva o dílo – Log management a SIEM

Číslo smlouvy Objednatele:

Číslo smlouvy Zhotovitele: [DOPLNÍ DODAVATEL]

uzavřená podle ustanovení § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“ nebo „**OZ**“).

Objednatel: Správa železnic, státní organizace

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn.
A 48384

Praha 1 - Nové Město, Dlážděná 1003/7, PSČ 110 00

IČO 70994234, DIČ CZ70994234

zastoupená **Bc. Jiřím Svobodou, MBA**, generálním ředitelem

(dále též jen „**Objednatel**“ nebo „**SŽ**“)

Zhotovitel: [DOPLNÍ DODAVATEL *jméno osoby/název firmy*]

[DOPLNÍ DODAVATEL *údaje o zápisu v evidenci*]

[DOPLNÍ DODAVATEL *sídlo*]

IČO [DOPLNÍ DODAVATEL], DIČ [DOPLNÍ DODAVATEL]

Bankovní spojení: [DOPLNÍ DODAVATEL]

Číslo účtu: [DOPLNÍ DODAVATEL]

[DOPLNÍ DODAVATEL *údaje o statutárním orgánu nebo jiné oprávněné osobě*]

(dále též jen „**Zhotovitel**“ nebo „**Dodavatel**“)

(dále jednotlivě též jen „**Strana**“ nebo společně „**Strany**“ a „**Smlouva**“)

Tato Smlouva byla uzavřena na základě výsledku zadávacího řízení veřejné zakázky s názvem „**Log management a SIEM**“, **ev. č. veřejné zakázky ve Věstníku veřejných zakázek:**

/ č.j. veřejné zakázky 61441/2023-SŽ-GR-O8 (dále jen „**Veřejná zakázka**“ a „**Zadávací řízení**“) Objednatel jako zadavatelem ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“), neboť nabídka Dodavatele podaná na Veřejnou zakázku (dále jen „**Nabídka**“) byla Objednatel vyhodnocena jako ekonomicky nejvýhodnější.

Jednotlivá ustanovení této Smlouvy tak budou vykládána s ohledem a v souladu se zadávacími podmínkami Veřejné zakázky. V případě kolize ustanovení obsažených v jednotlivých dokumentech smluvní dokumentace mají přednost ustanovení obsažená v následujících dokumentech v uvedeném pořadí (pokud není výslovně uvedeno jinak):

- 1) Vlastní text Smlouvy;
- 2) Přílohy č. 1 až 6 Smlouvy;
- 3) Příloha č. 7 Smlouvy – Zvláštní obchodní podmínky pro Zakázky v oblasti ICT (dále jen „**ZOP**“);
- 4) Příloha č. 8 Smlouvy – Obchodní podmínky ke Smlouvě o dílo (dále jen „**OOP**“);
- 5) Ostatní dokumenty zadávací dokumentace Veřejné zakázky či zmiňované ve Smlouvě.

Pokud nevyplývá ze Smlouvy jinak, mají pojmy s velkými počátečními písmeny význam definovaný v ZOP, nebo OOP. Pro vyloučení jakýchkoliv pochybností Strany uvádějí, že pokud je ve Smlouvě obsažen článek se shodným názvem jako v ZOP, OOP nebo jiném smluvním dokumentu, neznamená to, že by článek Smlouvy plně nahrazoval příslušné články v jiných smluvních dokumentech, pokud není výslovně uvedeno jinak; obdobné platí pro vztahy mezi jinými smluvními dokumenty.

1 Účel Smlouvy

- 1.1 Objednatel jako subjekt povinný v souladu s ustanoveními § 3 písm. c) a d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZoKB**“), musí provádět bezpečnostní opatření (§ 5 ZoKB) v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury. Jedním ze způsobů, jak naplnit tyto povinnosti, je implementace řešení Log management a SIEM, které bude zajišťovat jednotný sběr provozních a bezpečnostních událostí z prostředí SŽ, uchovávat je pro potřeby analýzy a archivovat je v souladu s legislativními požadavky.
- 1.2 Účelem této Smlouvy je tak zejména provedení Díla, tj. provedení Předmětu díla a poskytnutí souvisejících plnění v takovém rozsahu a takovým způsobem, aby minimálně po dobu trvání Smlouvy došlo k naplnění bezpečnostních požadavků, jejichž naplnění je provedením Díla sledováno.
- 1.3 Účelem této Smlouvy je to, aby bylo Dílo Zhotovitelem provedeno a po dobu trvání Smlouvy udržováno funkční v souladu s požadavky vyplývajícími z:
 - 1.3.1 právních předpisů;
 - 1.3.2 Smlouvy a jejích příloh;
 - 1.3.3 zadávací dokumentace Veřejné zakázky;
 - 1.3.4 Nabídky a
 - 1.3.5 Interních předpisů SŽ (dále jen „**Interní předpisy**“), přičemž se za Interní předpisy pro účely této Smlouvy považují interní předpisy SŽ, se kterými byl Zhotovitel prokazatelně seznámen. Součástí zadávací dokumentace Veřejné zakázky je interní předpis s názvem „Provozní politika prvků v působnosti systému řízení bezpečnosti informací“.

2 Předmět Smlouvy

- 2.1 Předmětem této Smlouvy je závazek Zhotovitele provést na svůj náklad a nebezpečí pro Objednatele řádně a včas Dílo a závazek Objednatele Dílo převzít a zaplatit Zhotoviteli Cenu díla a příslušnou DPH, a to vše za podmínek stanovených v této Smlouvě.
- 2.2 **Předmětem díla** je poskytnutí vymezených činností za účelem dodávky, implementace a podpory řešení Log management a SIEM, které bude zajišťovat jednotný sběr provozních a bezpečnostních událostí z prostředí SŽ, uchovávat je pro potřeby analýzy a archivovat je v souladu s legislativními požadavky. Bližší požadavky na Předmět díla jsou vymezeny zejména, nikoliv však výlučně, v části 2 a části 4 přílohy č. 1 *Specifikace plnění této Smlouvy* (dále jen „**Příloha č. 1**“).
- 2.3 Provedení Díla spočívá v provedení následujících **oblastí** dílčích činností ze strany Zhotovitele podrobně definovaných v části 2 a 4 Přílohy č. 1:

Etap

Etapa 1A

2.3.1 Před-implementační analýza dle části 2.3.1 a 4.1.1 Přílohy č. 1.

Etapa 1B

2.3.2 Instalace a konfigurace řešení, Dodávka technologií Log management a SIEM
Napojení určených zdrojů logů pro etapu 1 dle části 2.3.1, 2.4, 2.4.13 a 4.1.2 a 4.1.3 Přílohy č. 1.

Etapa 2

2.3.3 Napojení určených zdrojů logů pro etapu 2 dle části 2.3.2 a 4.1.3 Přílohy č. 1.

Etapa 3

2.3.4 Tvorba a optimalizace bezpečnostní/detekční politiky řešení dle části 2.3.3 a 4.1.4. Přílohy č. 1

2.3.5 Školení dle části 4.1.5 Přílohy č. 1.

Etapa 4

2.3.6 Napojení určených zdrojů logů pro etapu 4 dle části 2.3.4 a 4.1.3 Přílohy č. 1.

Etapa 5

2.3.7 Technická podpora servisního týmu SŽ dle části 2.3.5 a 4.2.1 Přílohy č. 1.

2.3.8 Údržba řešení dle části 2.3.5 a 4.2.2 Přílohy č. 1.

Etapa 6

2.3.9 Konzultace a rozvojové aktivity dle části 4.2.3 Přílohy č. 1.

3 Místo plnění

- 3.1 Místem plnění Smlouvy je především sídlo Objednatele a sídla jednotlivých organizačních složek Objednatele, nebo jakákoliv jiná místa, pokud je to potřebné či vhodné za účelem provedení Díla.
- 3.2 Přípravné práce je Zhotovitel oprávněn realizovat na svém vlastním technickém vybavení, což však nezakládá jakýkoliv nárok Zhotovitele na navýšení Ceny díla v souvislosti s následnou realizací Díla u Objednatele.

4 Doba plnění

- 4.1 Doba trvání Smlouvy činí 5 let a 4 měsíce (dále jen „**doba trvání Smlouvy**“) ode dne účinnosti Smlouvy. Tato Smlouva však nepozbyde účinnosti dříve, než za 5 let od ukončení etapy 1B podle přílohy č. 3 Smlouvy (dále jen „**Harmonogram**“).
- 4.2 Harmonogram předpokládá pro zahájení plnění Etapy 1B připravenost Platformy SŽ na straně Objednatele, přičemž tato podmínka bude splněna prohlášením Objednatele o připravenosti virtualizační platformy vůči Zhotoviteli.
- 4.3 Doba trvání Smlouvy nemá vliv na existenci práv a povinností Stran, která mají vzhledem ke své povaze a okolnostem trvat i po konci doby trvání Smlouvy.
- 4.4 Pokud není stanoveno jinak, je Zhotovitel povinen provádět Dílo v termínech uvedených v závazném harmonogramu realizace Díla obsaženém v Harmonogramu.

- 4.5 Žádná ze Stran není oprávněna jednostranně měnit termíny uvedené v Harmonogramu.

5 Cena díla

- 5.1 Celková cena za splnění závazku Zhotovitele provést Dílo v rozsahu dle Smlouvy, tj. Cena díla, je uvedena pod položkou Nabídková cena celkem v příloze č. 2 Smlouvy (dále jen „**Příloha č. 2**“).
- 5.2 Ceny, a to jak jednotkové ceny, tak nabídková cena celkem, obsažené v Příloze č. 2. Nabídková cena, jsou uvedeny jako maximální, nejvýše přípustné, nepřekročitelné a zahrnující veškeré náklady Zhotovitele nutné k řádnému a včasnému provedení Díla, resp. příslušného dílčího plnění (např. správní a místní poplatky, vedlejší náklady, náklady spojené s dopravou do místa plnění, včetně nákladů souvisejících s celními poplatky a s provedením všech zkoušek a testů prokazujících dodržení předepsané kvality a parametrů Předmětu plnění dle Smlouvy, náklady na licence apod. jsou všechny zahrnuty v cenách obsažených v Příloze č. 2).
- 5.3 Součástí Ceny díla jsou i náklady na dodávky a služby, které v zadávací dokumentaci Veřejné zakázky, Nabídce ani ve Smlouvě a jejích přílohách nejsou výslovně uvedeny, ale Zhotovitel jakožto odborník ví nebo má vědět, že jsou nezbytné pro řádné a včasné provedení Díla. Zhotovitel nese veškeré náklady nutné nebo účelně vynaložené při plnění závazku ze Smlouvy včetně správních poplatků.
- 5.4 Ceny obsažené v Příloze č. 2 jsou uvedeny bez DPH. V případě změny zákonné sazby DPH není třeba uzavírat dodatek ke Smlouvě, ledaže o to Objednatel požádá.
- 5.5 Zhotovitel odpovídá za to, že sazba DPH je stanovena v souladu s platnými právními předpisy.
- 5.6 Změna Ceny díla dle části 5 odst. 19.2 OOP se nepřipouští.

6 Platební podmínky

- 6.1 Zhotovitel je oprávněn doručit Objednateli Výzvu k úhradě v následujících platebních milnících, v níže definovaných výších a za níže vymezených podmínek:
- 6.1.1 První platební milník: Výzva k úhradě ve výši jednotkové ceny za položku v Příloze č. 2: E1 - Před-implementační analýza, Implementační služby (napojení určených zdrojů logů pro Etapu 1), E1 - Licence, údržba licencí a technická podpora výrobce na 60 měsíců, nebo subskripce licencí včetně údržby a technické podpory na 60 měsíců (celková cena za výčet licencí uvedených v Příloze č. 20 Zadávací dokumentace "Log management a SIEM dotazník", záložka Licence), E1 – Hardwarové prostředky, dodávané nad rámec specifikovaných Požadavků na služby Platformy SŽ, technická podpora výrobce HW na 60 měsíců, údržba a technická podpora HW dodavatele na 60 měsíců, a to nejdříve po akceptaci (bez výhrad) Etapy 1 (tedy Etapy 1A a Etapy 1B), která je tvořena činnostmi uvedenými v části 2.3.1., 2.4., 2.4.13, 4.1.1;4.1.2;4.1.3 Přílohy č. 1;
- 6.1.2 Druhý platební milník: Výzva k úhradě ve výši jednotkové ceny za položku v Příloze č. 2: E2 - Implementační služby (napojení určených zdrojů logů pro Etapu 2), a to nejdříve po akceptaci (bez výhrad) Etapy 2, která je tvořena činnostmi uvedenými v části 2.3.2 a 4.1.3 Přílohy č. 1;
- 6.1.3 Třetí platební milník: Výzva k úhradě ve výši jednotkové ceny za položku v Příloze č. 2: E3 – Tvorba a optimalizace bezpečnostní / detekční politiky řešení, Školení, a to nejdříve po akceptaci (bez výhrad) Etapy 3, která je tvořena činnostmi uvedenými v části 2.3.3, 4.1.4 a 4.1.5. Přílohy č. 1;

- 6.1.4 Čtvrtý platební milník: Výzva k úhradě ve výši jednotkové ceny za položku v Příloze č. 2: E4 - Implementační služby (napojení určených zdrojů logů pro Etapu 4), a to nejdříve po akceptaci (bez výhrad) Etapy 4, která je tvořena činnostmi uvedenými v části 2.3.2 a 4.1.3 Přílohy č. 1;
- 6.2 Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě za poskytování služeb Technická podpora servisního týmu SŽ dle čl. 2.3.5 a 4.2.1 Přílohy č. 1 a čl. 11 této Smlouvy, a Údržba řešení dle čl. v části 2.3.5 a 4.2.2 Přílohy č. 1 této Smlouvy, a to opakovaně po dobu trvání Smlouvy po uplynutí každého 1 měsíce ode dne akceptace (bez výhrad) Etapy 1B. Každá Výzva k úhradě dle předchozí věty může být vystavena ve výši jednotkové ceny za položku dle Přílohy č. 2 této Smlouvy: Technická podpora servisního týmu SŽ, údržba řešení.
- 6.3 Zhotovitel je dále oprávněn doručit Objednateli Výzvu k úhradě po akceptaci (bez výhrad) každého plnění na základě Objednávky Konzultací a rozvojových aktivit dle čl. 12 této Smlouvy, a to ve výši součinu počtu MD dle skutečně provedených MD (nejvýše dle Objednávky) a ceny za jednu MD dle příslušné položky ceny Konzultace a rozvojové aktivity uvedené Příloze č. 2 této Smlouvy.
- 6.4 Výzva k úhradě musí být fakturou nebo daňovým dokladem. Kromě náležitostí účetního či daňového dokladu musí být Výzva k úhradě označena registračním číslem projektu: ... Pokud je Výzva k úhradě hrazena z více zdrojů, budou na ní uvedena všechna čísla projektů. Objednatel je oprávněn čísla projektu aktualizovat v průběhu trvání této Smlouvy a Zhotovitel je povinen tuto skutečnost akceptovat a zohlednit v rámci prováděné fakturace.
- 6.5 Výzvu k úhradě doručí Zhotovitel Objednateli jedním z následujících způsobů:
- 6.5.1 V listinné podobě na adresu:
- Správa železnic, státní organizace
Centrální finanční účtárna Čechy
Náměstí Jana Pernera 217
530 02 Pardubice
- 6.5.2 V elektronické podobě na adresu:
- ePodatelnaCFU@spravazeleznic.cz
- 6.5.3 prostřednictvím datové schránky:
- uccchjm
- 6.6 Splatnost každé Výzvy k úhradě se sjednává na 60 kalendářních dnů od jejího doručení Objednateli. V případě, že Výzva k úhradě nebude mít odpovídající náležitosti, je Objednatel oprávněn ve lhůtě splatnosti ji vrátit Zhotoviteli s vytknutím nedostatků, aniž by se dostal do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od okamžiku doručení opravené či doplněné Výzvy k úhradě Objednateli.
- 6.7 Zhotovitel, poskytovatel zdanitelného plnění, je povinen bezprostředně, nejpozději do 2 (slovy: dvou) pracovních dnů od zjištění svého úpadku, popř. od vydání rozhodnutí správce daně, že je Zhotovitel nespolehlivým plátcem dle § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „ZDPH“), oznámit takovou skutečnost prokazatelně Objednateli, příjemci zdanitelného plnění. Porušení této povinnosti je Stranami považováno za podstatné porušení Smlouvy.
- 6.8 Zhotovitel se zavazuje, že bankovní účet jím určený pro zaplacení jakéhokoliv závazku Objednatele na základě Smlouvy bude od data podpisu Smlouvy do ukončení její platnosti zveřejněn způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 ZDPH, v

opačném případě je Zhotovitel povinen sdělit Objednateli jiný bankovní účet řádně zveřejněný ve smyslu § 96 ZDPH.

- 6.9 Strany se dohodly na tom, že Zhotovitel není oprávněn činit jednostranná započtení svých pohledávek vzniklých na základě Smlouvy či v souvislosti s ní vůči jakýmkoliv pohledávkám Objednatele. Pohledávky a nároky Zhotovitele vzniklé na základě Smlouvy či v souvislosti s ní nesmějí být Zhotovitelem postoupeny třetím osobám, zastaveny, nebo s nimi nesmí být jinak disponováno bez předchozího písemného souhlasu Objednatele (zahrnuje i zákaz Zhotovitele postoupit Smlouvu). Jakýkoliv právní úkon učiněný Zhotovitelem v rozporu s tímto ustanovením bude považován za podstatné porušení Smlouvy.
- 6.10 Zhotovitel se rovněž zavazuje zajistit řádné a včasné plnění finančních závazků vůči svým Poddodavatelům, prostřednictvím kterých bude realizovat Dílo, resp. jeho část dle této Smlouvy. Za řádné a včasné plnění dle předcházející věty se považuje plné uhrazení Poddodavatelem řádně vystavených faktur za předmět smlouvy, resp. jeho část, a to vždy do 60 kalendářních dnů od obdržení platby ze strany Objednatele za konkrétní plnění předmětu smlouvy, resp. jeho části.

7 Akceptační řízení

- 7.1 Akceptačnímu řízení dle části 8 ZOP a tohoto článku Smlouvy podléhají Etapy definované v čl. 2 odst. 2.3.1 až 2.3.9. této Smlouvy, tj. Etapa 1A, Etapa 1B, Etapa 2, Etapa 3, Etapa 4, Etapa 5 a Etapa 6. Pro vyloučení všech pochybností Strany výslovně uvádějí, že Etapa 1A, Etapa 1B, Etapa 2, Etapa 3, Etapa 4, Etapa 5 a Etapa 6 podléhají samostatnému Akceptačnímu řízení.
- 7.2 Každá Fáze plnění podléhají samostatnému Akceptačnímu řízení se považuje za ukončenou akceptací (bez výhrad) posledního dílčího plnění uvedeného pro příslušnou Etapu v části 2 a 4 Přílohy č. 1 této Smlouvy. Akceptační kritéria pro každou dílčí část jednotlivých Etap vyplývají z části 2 a 4 Přílohy č. 1 této Smlouvy, kdy Dodavatel předá Objednateli všechny části plnění uvedené v kategorii „Výstupy“. U Etapy 5 předá Dodavatel Objednateli vždy do 5 dnů od skončení příslušného měsíce poskytování služeb měsíční výkaz shrnující poskytnutí dané služby za tento měsíc.
- 7.3 Zhotovitel bere na vědomí, že v rámci Předmětu díla může dojít k upřesnění Předmětu díla, resp. Akceptačních kritérií jednotlivých Etap. Vzhledem ke skutečnosti uvedené v předchozí větě nemohou být veškerá Akceptační kritéria vymezena zcela vyčerpávajícím způsobem. Zhotovitel proto bere na vědomí skutečnosti uvedené v tomto odstavci a zavazuje se v tomto ohledu postupovat v souladu s principy „best practice“ a zohledňovat veškeré připomínky Objednatele, které lze s ohledem na účel Smlouvy považovat za oprávněné. Zhotovitel dále bere na vědomí, že vzhledem ke skutečnostem uvedeným v tomto odstavci mohou být v rámci Akceptačního řízení vzneseny Objednatelem výhrady, jejichž povaha bude bránit akceptaci a jejichž důsledkem tak může být prodloužení doby Akceptačního řízení. Objednatel se zavazuje poskytnout Zhotoviteli součinnost při projednání připomínek k Předmětu díla i ve fázích přípravy.
- 7.4 Akceptačnímu řízení dle části 8 ZOP a tohoto článku Smlouvy podléhají rovněž práce provedené na základě Objednávek Konzultací a rozvojových aktivit dle článku 12 Smlouvy. Akceptační kritéria vyplývají ze specifikace prací uvedených v Objednávce.
- 7.5 Posuzování jakýchkoliv Akceptačních kritérií je nutno provádět s ohledem na účel Smlouvy.

8 Licenční ujednání

- 8.1 Pokud jsou výstupy dílčích činností ze strany Zhotovitele podrobně definované v části 4 Přílohy č. 1 této Smlouvy, Autorským dílem, uplatní se čl. 6.2. ZOP.

- 8.2 Zhotovitel prohlašuje a zavazuje se, že je a bude plně oprávněn disponovat právy duševního vlastnictví týkajícími se Díla, včetně práv autorských, a zavazuje se zajistit řádné a nerušené užívání Díla Objednatel, včetně zajištění souhlasů všech nositelů práv duševního vlastnictví. Zhotovitel je povinen Objednateli uhradit jakékoli majetkové a nemajetkové újmy, vzniklé v důsledku toho, že by Objednatel nemohl Dílo nebo jakoukoli jeho část užívat řádně a nerušeně.
- 8.3 Zhotovitel se zavazuje, že při provádění Díla neporuší práva třetích osob, která těmto osobám mohou plynout z práv k duševnímu vlastnictví, a to po celou dobu trvání autorských práv k Dílu. Za případné porušení této povinnosti, a to i nastalé v průběhu užívání Díla Objednatel, bude vůči takovým třetím osobám odpovědný výhradě Zhotovitel. Pokud budou práva třetích osob váznout na podkladech, materiálech a dalších předmětech, které Zhotoviteli poskytne Objednatel bez toho, aby jej na tyto skutečnosti upozornil, ponese odpovědnost za případné porušení práv třetích osob Objednatel.

9 Školení

- 9.1 Objednatel požaduje provedení školení ze strany Zhotovitele, jehož parametry jsou podrobněji vymezeny v čl. 4.1.5 Přílohy č. 1 této Smlouvy.

10 Helpdesk

- 10.1 Zhotovitel se zavazuje nejpozději do dne účinnosti Smlouvy založit a po celou dobu trvání Smlouvy udržovat v provozu Helpdesk, a to za podmínek dle části 10 ZOP.
- 10.2 Zhotovitel se zavazuje zajišťovat Helpdesk v **Režimu 1** ve smyslu části 10 ZOP.
- 10.3 Helpdesk bude provozován ve třetí **úrovni (L3)** podpory ve smyslu části 10 ZOP.

11 Technická podpora servisního týmu SŽ a Údržba řešení

- 11.1 Zhotovitel se zavazuje v souladu s částí 4.2.1 a 4.2.2. Přílohy č. 1 této Smlouvy poskytovat Objednateli Technickou podpora servisního týmu SŽ a Údržbu řešení, a to ode dne akceptace (bez výhrad) Etapy B1 po dobu 60 měsíců.
- 11.2 Technická podpora servisního týmu SŽ a Údržba řešení spočívá zejména v přijímání hlášení o Incidentech přes Helpdesk a jejich následném vyřešení v souladu s podmínkami této Smlouvy.
- 11.3 Způsob nahlášení Incidentu je stanoven v části 11 ZOP, přičemž Ohlašovatel určí kategorii Incidentu dle odst. 1.1.19 ZOP. Určení kategorie Incidentu může být změněno, pokud Zhotovitel prokáže, že kategorie Incidentu je jiná.
- 11.4 Incidentsy a Požadavky budou řešeny podle **servisního modelu B1** vymezeného v části 12 ZOP.

12 Služby Konzultace a rozvojové aktivity

- 12.1 Zhotovitel se zavazuje poskytovat Služby konzultace a rozvojové aktivity na vyžádání, které jsou blíže vymezeny v části 4.2.3 Přílohy č. 1 této Smlouvy.
- 12.2 Maximální souhrn Služeb konzultace a rozvojových aktivit na vyžádání činí 250 MD za celou dobu trvání Smlouvy ode dne účinnosti Smlouvy.
- 12.3 Objednatel v případě zájmu o provedení prací v rámci Služeb konzultace a rozvojových aktivit na vyžádání doručí Zhotoviteli objednávku prostřednictvím e-mailu Kontaktních osob uvedených v čl. 14 této Smlouvy se specifikací požadovaných prací v části 4.2.3 Přílohy č. 1 této Smlouvy, termínem provedení těchto prací a předpokládanou časovou náročností vyjádřenou v MD (dále jen „**Objednávka**“).

- 12.4 Zhotovitel se zavazuje bez zbytečného odkladu projednat s Objednatelům své případné připomínky k Objednávce, přičemž je povinen postupovat v souladu s principy „best practice“ a s ohledem na účel Smlouvy. Objednatel je povinen oprávněné připomínky Zhotovitele zohlednit v obsahu Objednávky.
- 12.5 V případě, že Zhotovitel (již) nemá žádné oprávněné připomínky k Objednávce, je povinen Objednávku nejpozději do 3 pracovních dnů písemně přijmout prostřednictvím e-mailu Kontaktních osob uvedených v čl. 14 této Smlouvy. Příjmutím Objednávky vzniká Zhotoviteli povinnost provést v Objednávce specifikované práce, a to při dodržení stanovených termínů a stanovené časové náročnosti vyjádřené v MD.
- 12.6 Na provedení prací dle Objednávky a s tím souvisejícího práva a povinnosti Stran se v rozsahu, v jakém je to možné, použijí ustanovení této Smlouvy. Zhotovitel je tak především, nikoliv však výlučně, povinen předložit provedené práce k Akceptačnímu řízení a poskytnout ve vztahu k těmto pracím Objednateli licenci či jiná práva z duševního vlastnictví v rozsahu dle čl. 7.1 této Smlouvy.

13 Účast poddodavatelů a realizační tým

- 13.1 Zhotovitel je oprávněn plnit tuto Smlouvu výlučně prostřednictvím Poddodavatelů uvedených v příloze č. 6 této Smlouvy – Seznam poddodavatelů.
- 13.2 Před zapojením nového Poddodavatele do plnění Smlouvy musí být Objednateli předložen nový seznam poddodavatelů, který bude tvořit přílohu č. 6 této Smlouvy, a tento seznam musí být Objednatelům písemně schválen. Tím nejsou dotčeny dodatečné podmínky pro změnu Poddodavatele, jehož prostřednictvím Zhotovitel prokazoval kvalifikaci ve Veřejné zakázce, uvedené v části 13 ZOP.
- 13.3 Seznam členů realizačního týmu je Přílohou č. 9 této Smlouvy. Pravidla pro realizační tým se řídí částí 14 ZOP.

14 Komunikace stran

- 14.1 Každá ze Stran jmenuje Kontaktní osoby, které budou vystupovat jako zástupci Stran a prostřednictvím kterých bude probíhat veškerá komunikace předpokládaná touto Smlouvou nebo ZOP. Kontaktní osoby zastupují Stranu ve smluvních a technických záležitostech souvisejících s plněním předmětu Smlouvy, zejména podávají a přijímají informace o průběhu plnění Smlouvy (dále jen „**Kontaktní osoby**“).
- 14.2 Kontaktními osobami za Objednatelē jsou:
- ve věcech smluvních: [BUDE DOPLNĚNO JMÉNO, TEL., EMAIL]
 - ve věcech technických: [BUDE DOPLNĚNO JMÉNO, TEL., EMAIL]
 - ve věcech kybernetické bezpečnosti: [BUDE DOPLNĚNO JMÉNO, TEL., EMAIL]
- Kontaktními osobami za Zhotovitelē jsou:
- ve věcech smluvních: [DOPLNÍ DODAVATEL JMÉNO, TEL., EMAIL]
 - ve věcech technických: [DOPLNÍ DODAVATEL JMÉNO, TEL., EMAIL]
 - ve věcech kybernetické bezpečnosti: [DOPLNÍ DODAVATEL JMÉNO, TEL., EMAIL]
- 14.3 Každá ze Stran má právo změnit jí jmenované Kontaktní osoby, musí však o každé změně vyrozumět písemně druhou Stranu. Změna Kontaktních osob je vůči druhé Straně účinná okamžikem, kdy o ní byla písemně vyrozuměna; v případě změny Kontaktní osoby není třeba uzavírat dodatek ke Smlouvě.

15 Smluvní pokuty

- 15.1 Objednatel je povinen uhradit smluvní pokutu za překročení nároků řešení na Požadavky na služby Platformy SŽ (příloha č. 5), které dodavatel definuje v listu „Požadavky“ dle této přílohy, a to ve výši 150,00 Kč za každý bod nad celkový počet bodů uvedených v buňce C14 na řádku označeném Dílčí body hodnotícího kritéria "Požadavky na služby Platformy SŽ" dle požadavků na služby Platformy SŽ.
- 15.2 Překročení nároků systému na Požadavky na služby Platformy SŽ je Objednatel oprávněn posuzovat kdykoli po dobu trvání účinnosti této Smlouvy, i kdykoliv po jejím skončení.
- 15.3 Jestliže Objednatel uplatní nárok na smluvní pokutu dle odstavce 15.1 této Smlouvy a následně by mu vzniklo právo požadovat vyšší smluvní pokutu dle odstavce 15.1 této Smlouvy, má Objednatel právo požadovat rozdíl mezi touto vyšší smluvní pokutou a nižší smluvní pokutou již dříve uplatněnou.
- 15.4 Cenou pro účely stanovení výše smluvních pokut dle části 16 ZOP a části 20 OOP se rozumí Cena díla, není-li výslovně stanoveno jinak.

16 Ukončení smluvního vztahu

- 16.1 Objednatel je oprávněn odstoupit od Smlouvy, pokud dojde k významné změně ovládnání Dodavatele podle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, nebo změně vlastnictví zásadních aktiv, využívaných Dodavatelem k plnění Smlouvy a změně oprávnění nakládat s těmito aktivy, či dojde ke změně ekvivalentní změnám výše uvedeným a tato změna bude Objednatelem vyhodnocena jako riziko bezpečnosti informací, které nelze odstranit jiným opatřením; toto ustanovení se uplatní i pro případ, že Dodavatel o takových změnách dopředu a včas neinformuje Objednatele.
- 16.2 Dodavatel se zavazuje dle pokynů Objednatele v souvislosti s ukončením smluvního vztahu založeného touto Smlouvou (z jakéhokoli důvodu) provádět činnosti spočívající v součinnosti při ukončení této Smlouvy (exit plán), a to při přípravě a předání novému Dodavateli, nebo Objednateli.
- 16.3 Činnosti dle čl. 16.2 této Smlouvy budou provedeny v souladu s výstupem předimplementační analýzy dle čl. 4.1.1 Přílohy č. 1 této Smlouvy a jsou již zahrnuty v Ceně díla.
- 16.4 Dodavatel se zavazuje součinnost dle článku 16.2 této Smlouvy poskytovat s odbornou péčí, zodpovědně a do doby úplného převzetí novým dodavatelem, nebo Objednatelem.
- 16.5 Nesplnění kteréhokoliv požadavku na technické funkcionality řešení uvedené v kapitole 2.4. Přílohy č. 1 a v příloze č. 4 této smlouvy „Log management a SIEM dotazník“ a funkcionality uvedených v této Smlouvě bude to považováno za hrubé porušení povinností a bude důvodem pro odstoupení od této Smlouvy.
- 16.6 Další pravidla pro ukončení smluvního vztahu stanoví část 18 ZOP.

17 Kybernetická bezpečnost

- 17.1 Zhotovitel se zavazuje k zachovávaní požadavků kybernetické bezpečnosti zejména dle části 20 ZOP.
- 17.2 Zhotovitel je významným dodavatelem, zavazuje se tedy i k zachovávaní požadavků kybernetické bezpečnosti dle části 20 ZOP vztahujících se k významným dodavatelům.

18 Ochrana osobních údajů

- 18.1 Pokud bude v rámci plnění této Smlouvy docházet ke zpracování osobních údajů, zavazuje se Zhotovitel dodržovat opatření dle části 21 ZOP.

19 Ochrana důvěrných informací

19.1 Zhotovitel se zavazuje k ochraně důvěrných informací dle části 22 ZOP.

20 Střet zájmů, povinnosti Zhotovitele v souvislosti s konfliktem na Ukrajině

20.1 Zhotovitel prohlašuje, že není obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „**Zákon o střetu zájmů**“), nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti, a že žádní poddodavatelé, jimiž prokazoval kvalifikaci v zadávacím řízení na zadání Veřejné zakázky, nejsou obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.

20.2 Zhotovitel prohlašuje, že on, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost byla využita ve smyslu evropských směrnic o zadávání veřejných zakázek, nejsou osobami:

20.2.1 dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů, jimž se zakazuje zadat nebo dále plnit jakoukoli veřejnou zakázku nebo koncesní smlouvu spadající do oblasti působnosti směrnic o zadávání veřejných zakázek, jakož i čl. 10 odst. 1, 3, odst. 6 písm. a) až e), odst. 8, 9 a 10, článků 11, 12, 13 a 14 směrnice 2014/23/EU, čl. 7 písm. a) až d), článku 8, čl. 10 písm. b) až f) a h) až j) směrnice 2014/24/EU, článku 18, čl. 21 písm. b) až e) a g až i), článků 29 a 30 směrnice 2014/25/EU a čl. 13 písm. a) až d), f) až h) a j) směrnice 2009/81/ES a hlavy VII nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046,

20.2.2 dle článku 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů, a dalších prováděcích předpisů k tomuto nařízení Rady (EU) č. 269/2014 (dále jen „**Sankční seznamy**“).

20.3 Je-li Zhotovitelem sdružení více osob, platí podmínky dle odstavce 20.1 a 20.2 této Smlouvy také jednotlivě pro všechny osoby v rámci Zhotovitele sdružené, a to bez ohledu na právní formu tohoto sdružení.

20.4 Přestane-li Zhotovitel nebo některý z jeho poddodavatelů nebo jiných osob, jejichž způsobilost byla využita ve smyslu evropských směrnic o zadávání veřejných zakázek, splňovat podmínky dle tohoto článku Smlouvy, oznámí tuto skutečnost bez zbytečného odkladu, nejpozději však do 3 pracovních dnů ode dne, kdy přestal splňovat výše uvedené podmínky, Objednateli.

20.5 Zhotovitel se dále zavazuje postupovat při plnění této Smlouvy v souladu s Nařízením Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vzhledem k situaci v Bělorusku a k zapojení Běloruska do ruské agrese proti Ukrajině, ve znění pozdějších předpisů, a dalších prováděcích předpisů k tomuto nařízení Rady (EU) č. 269/2014.

20.6 Zhotovitel se dále ve smyslu článku 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů, zavazuje, že finanční prostředky ani hospodářské zdroje, které obdrží od Objednatele na základě této Smlouvy a jejích případných dodatků, nepřístupní přímo ani nepřímo fyzickým nebo právnickým osobám, subjektům či orgánům s nimi spojeným uvedeným v Sankčních seznamech, nebo v jejich prospěch.

- 20.7 Ukáží-li se prohlášení Zhotovitele dle odstavce 20.1 a 20.2 této Smlouvy jako nepravdivá nebo poruší-li Zhotovitel svou oznamovací povinnost dle odstavce 20.4. nebo povinnosti dle odstavců 20.5 nebo 20.6 této Smlouvy, je Objednatel oprávněn odstoupit od této Smlouvy. Zhotovitel je dále povinen zaplatit za každé jednotlivé porušení povinností dle předchozí věty smluvní pokutu ve výši 5 % procent z Ceny díla (Cena bez DPH) sjednané dle této Smlouvy. Ustanovení § 2004 odst. 2 Občanského zákoníku a § 2050 Občanského zákoníku se nepoužijí.

21 Přímé platby poddodavatelům

- 21.1 Zhotovitel je povinen uhradit své závazky vůči poddodavatelům ve sjednané výši za sjednaných podmínek.
- 21.2 Objednatel si v souladu s § 106 ZZVZ vyhrazuje možnost úhrady splatných částek odpovídajícím plněním poskytnutých ze strany poddodavatele, a to na základě písemné žádosti poddodavatele, jestliže je Zhotovitel v prodlení s úhradou příslušné částky poddodavateli po dobu nejméně 30 dnů.
- 21.3 Poddodavatel může Objednatele požádat o úhradu splatné částky pouze za takové plnění, které již bylo poskytnuto.
- 21.4 Přímá platba poddodavateli bude Objednatelem provedena na základě oznámení vystaveného poddodavatelem Objednateli, které bude obsahovat informaci o výši částky, která má být přímo uhrazena poddodavateli (dále jen „**částka k úhradě**“) a podloženou kopií faktury vystavené poddodavatelem Zhotoviteli se všemi zákonem požadovanými náležitostmi. Nedílnou součástí faktury bude i kopie dokladu o existujícím závazku mezi Zhotovitelem a poddodavatelem, výše sjednané ceny (případně cen dílčích plnění) ve vazbě na plnění předmětu této Smlouvy a informace o tom, kdy byla částka, kterou měl Zhotovitel poddodavateli uhradit, splatná.
- 21.5 Částka k úhradě nesmí být vyšší než částka odpovídající skutečně poskytnutému plnění.
- 21.6 Objednatel informuje Zhotovitele bez zbytečného odkladu o skutečnosti, že obdržel oznámení poddodavatele k přímé úhradě poddodavateli. V případě, že Zhotovitel do 10 dnů ode dne obdržení této informace od Objednatele neprokáže, že tvrzení uváděná poddodavatelem v žádosti o přímou platbu jsou nesprávná, má se za to, že s provedením přímé úhrady poddodavateli souhlasí.
- 21.7 Splatnost částky k úhradě činí 60 dnů ode dne doručení žádosti poddodavatele k přímé úhradě. Objednatel je oprávněn před uplynutím lhůty splatnosti vrátit oznámení, které neobsahuje požadované náležitosti nebo obsahuje nesprávné údaje. Objednatel je rovněž oprávněn vrátit poddodavateli oznámení v případě, že Zhotovitel prokázal, že tvrzení poddodavatele uvedená v oznámení jsou nesprávná. Oprávněným vrácením oznámení přestává běžet lhůta splatnosti.
- 21.8 V případě, že částka k úhradě již byla uhrazena Zhotoviteli, Objednatel ji uhradí poddodavateli, a následně bude o částku k úhradě snížena celková odměna Zhotovitele, a to formou započtení proti pohledávce nebo pohledávkám Zhotovitele vzniklých na základě plnění této Smlouvy. O zápočtu proti pohledávce Zhotovitele musí Objednatel Zhotovitele písemně informovat. Není-li již budoucí platba, kterou by Objednatel mohl započíst proti své pohledávce vůči Zhotoviteli, představuje částka k úhradě výši smluvní pokuty za nesplnění povinnosti dle čl. 21.1 této Smlouvy a Zhotovitel se zavazuje tuto smluvní pokutu uhradit nejpozději do 15 dnů ode dne doručení výzvy k zaplacení.

22 Další povinnosti Zhotovitele

- 22.1 Zhotovitel je povinen uchovat veškerou dokumentaci související s plněním Smlouvy na veřejnou zakázku včetně účetních dokladů minimálně do 31. 12. 2035.
- 22.2 Zhotovitel je povinen minimálně do 31. 12. 2035 poskytovat požadované informace a dokumentaci související s plněním Smlouvy zaměstnancům nebo zmocněncům pověřených orgánů (Centra, Ministerstvo pro místní rozvoj ČR, Ministerstvo financí ČR, Evropská komise, Evropský účetní dvůr, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.
- 22.3 Zhotovitel je povinen při plnění předmětu plnění Smlouvy dodržovat pracovněprávní předpisy, a to zejména, nikoliv však výlučně, předpisy upravující mzdy zaměstnanců, pracovní dobu, dobu odpočinku mezi směnami, placené přesčasy, bezpečnost práce apod. Zhotovitel je dále povinen zajistit férové pracovní podmínky a odpovídající úroveň bezpečnosti práce pro všechny osoby podílející se na plnění Smlouvy. Zhotovitel se zavazuje výše uvedené zajistit i u svých poddodavatelů.
- 22.4 Plnění povinností dle čl. 22.3 Smlouvy je Zhotovitel povinen prokázat kdykoli do 5 pracovních dnů od doručení písemné výzvy Objednatele, a to prostřednictvím všech potřebných dokladů dle aktuálních právních předpisů, resp. též s příslušnými výstupy ze mzdového a účetního systému Zhotovitele.

23 Závěrečná ujednání

- 23.1 Strany berou na vědomí, že tato Smlouva podléhá uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „**ZRS**“), a současně souhlasí se zveřejněním údajů o identifikaci Stran, předmětu Smlouvy, jeho ceně či hodnotě a datu uzavření této Smlouvy.
- 23.2 Zaslání Smlouvy správci registru smluv k uveřejnění v registru smluv zajišťuje obvykle Objednatel. Nebude-li tato Smlouva zaslána k uveřejnění a/nebo uveřejněna prostřednictvím registru smluv, není žádná ze Stran oprávněna požadovat po druhé Straně náhradu škody ani jiné újmy, která by jí v této souvislosti vznikla nebo vzniknout mohla.
- 23.3 Strany výslovně prohlašují, že údaje a další skutečnosti uvedené v této Smlouvě, vyjma částí označených ve smyslu následujícího odstavce této Smlouvy, nepovažují za obchodní tajemství ve smyslu ustanovení § 504 Občanského zákoníku (dále jen „**obchodní tajemství**“), a že se nejedná ani o informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS.
- 23.4 Jestliže Strana označí za své obchodní tajemství část obsahu Smlouvy, která v důsledku toho bude pro účely uveřejnění Smlouvy v registru smluv znečitelněna, nese tato Strana odpovědnost, pokud by Smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, která ze stran Smlouvu v registru smluv uveřejnila. S částmi Smlouvy, které druhá Strana neoznačí za své obchodní tajemství před uzavřením této Smlouvy, nebude Objednatel jako s obchodním tajemstvím nakládat a ani odpovídat za případnou škodu či jinou újmu takovým postupem vzniklou. Označením obchodního tajemství ve smyslu předchozí věty se rozumí doručení písemného oznámení druhé Strany Objednateli obsahujícího přesnou identifikaci dotčených částí Smlouvy včetně odůvodnění, proč jsou za obchodní tajemství považovány. Druhá Strana je povinna výslovně uvést, že informace, které označila jako své obchodní tajemství, naplňují současně všechny definiční znaky obchodního tajemství, tak jak je vymezeno v ustanovení § 504

Občanského zákoníku, a zavazuje se neprodleně písemně sdělit Objednateli skutečnost, že takto označené informace přestaly naplňovat znaky obchodního tajemství.

- 23.5 Osoby uzavírající tuto Smlouvu za Strany souhlasí s uveřejněním svých osobních údajů, které jsou uvedeny v této Smlouvě, spolu se Smlouvou v registru smluv. Tento souhlas je udělen na dobu neurčitou.
- 23.6 Tato Smlouva je vyhotovena v elektronické podobě, přičemž obě Strany obdrží její elektronický originál opatřený elektronickými podpisy. V případě, že tato Smlouva z jakéhokoli důvodu nebude vyhotovena v elektronické podobě, bude sepsána ve třech vyhotoveních, přičemž jedno vyhotovení obdrží Dodavatel a dvě vyhotovení Objednatel.
- 23.7 Veškerá práva a povinnosti Stran vyplývající ze Smlouvy se řídí českým právním řádem.
- 23.8 Smluvní vztahy neupravené Smlouvou se řídí Občanským zákoníkem a dalšími právními předpisy.
- 23.9 Všechny spory vznikající ze Smlouvy a v souvislosti s ní budou dle vůle Stran rozhodovány soudy České republiky, jakožto soudy výlučně příslušnými.
- 23.10 Je-li nebo stane-li se jakékoli ustanovení Smlouvy neplatným, nezákonným nebo nevynutitelným, netýká se tato neplatnost a nevynutitelnost zbývajících ustanovení Smlouvy. Strany se tímto zavazují nahradit do 5 (slovy: pěti) pracovních dnů po doručení výzvy druhé Strany jakékoli takové neplatné, nezákonné nebo nevynutitelné ustanovení ustanovením, které je platné, zákonné a vynutitelné a má stejný nebo alespoň podobný obchodní a právní význam.
- 23.11 Smlouvu lze měnit pouze písemnými dodatky.
- 23.12 Tato Smlouva nabývá platnosti okamžikem podpisu poslední ze Stran. Je-li Smlouva uveřejňována v registru smluv, nabývá účinnosti dnem uveřejnění v registru smluv, jinak je účinná od okamžiku uzavření.

Přílohy

1. Specifikace plnění této Smlouvy (*jedná se o přílohu č. 1 zadávací dokumentace k Veřejné zakázce – Technická specifikace, Přílohu č. 2 zadávací dokumentace – Analýza prostředí – Architektura prostředí SŽ a Přílohu č. 3 Analýza prostředí – Popis prostředí sítě UAS*)
2. Specifikace nabídkové ceny (bude doplněno v souladu s Nabídkou Dodavatele podle Dodavatelem vyplněného vzoru obsaženého v příloze č. 9 zadávací dokumentace k Veřejné zakázce – Formulář pro vyplnění nabídkové ceny)
3. Harmonogram (Příloha č. 5 zadávací dokumentace)
4. Log management a SIEM dotazník (Příloha č. 20 zadávací dokumentace)
5. Požadavky na služby Platformy SŽ (Příloha č. 19 zadávací dokumentace)

6. Seznam poddodavatelů (bude doplněno v souladu s Nabídkou Dodavatele podle Dodavatelem vyplněného vzoru obsaženého v příloze č. 15 zadávací dokumentace k Veřejné zakázce – Vzor Seznamu Poddodavatelů)
7. Zvláštní obchodní podmínky pro Zakázky v oblasti ICT
8. Obchodní podmínky ke Smlouvě o dílo
9. Realizační tým (bude doplněno v souladu s Nabídkou Dodavatele podle Dodavatelem vyplněného vzoru obsaženého v příloze č. 8 Zadávací dokumentace – Seznam členů realizačního týmu)
10. Platforma 2.0 (*jedná se o přílohu č. 4 zadávací dokumentace k Veřejné zakázce – Platforma 2.0*)
11. Plná moc (pouze v případě zastoupení Dodavatele osobou na základě plné moci)

 Za Objednatele:

Za Dodavatele:

.....
Bc. Jiří Svoboda, MBA
generální ředitel

.....
[DOPLNÍ DODAVATEL]

Zvláštní obchodní podmínky pro Zakázky v oblasti ICT

OBSAH

1. VÝKLAD POJMŮ.....	2
2. DOBA A MÍSTO PLNĚNÍ.....	7
3. PRÁVA A POVINNOSTI OBOU STRAN	7
4. POVINNOSTI DODAVATELE.....	8
5. POVINNOSTI OBJEDNATELE	8
6. LICENČNÍ UJEDNÁNÍ	9
7. ZDROJOVÝ KÓD A DOKUMENTACE	11
8. AKCEPTAČNÍ ŘÍZENÍ	12
9. ŠKOLENÍ.....	13
10. HELPDESK.....	14
11. NAHLÁŠENÍ INCIDENTU	15
12. SERVISNÍ MODELY	15
13. ÚČAST PODDODAVATELŮ.....	17
14. REALIZAČNÍ TÝM.....	17
15. KOMUNIKACE STRAN	17
16. SMLUVNÍ POKUTY.....	18
17. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ	19
18. UKONČENÍ SMLUVNÍHO VZTAHU	20
19. ZMĚNY SMLOUVY A ZMĚNOVÉ ŘÍZENÍ	21
20. KYBERNETICKÁ BEZPEČNOST	22
21. OCHRANA OSOBNÍCH ÚDAJŮ.....	25
22. OCHRANA DŮVĚRNÝCH INFORMACÍ.....	27

1. VÝKLAD POJMŮ

- 1.1. **Akceptační kritéria** představují podmínku nebo vlastnost výstupu provádění Plnění dle Smlouvy, která musí být splněna, aby bylo Plnění dle Smlouvy provedeno, přičemž Akceptační kritéria jsou uvedena v Příloze Smlouvy, která obsahuje specifikaci Plnění (dále jen „**Specifikace Plnění**“).
- 1.2. **Akceptační protokol** je protokol, který jsou zavázáni podepsat Objednatel i Dodavatel po provedení všech nezbytných činností v rámci Akceptačního řízení, potvrzující provedení výstupu provádění Plnění anebo výsledek Testů výstupů provádění Plnění. Protokol je připravený ze strany Dodavatele a následně upravený a vyplněný Objednatel. Akceptační protokol obsahuje:
 - a. Specifikaci provedeného Plnění;
 - b. Akceptační kritéria;
 - c. informace o průběhu Testů, jsou-li prováděny;
 - d. další informace a dokumenty nezbytné pro provedení Akceptačního řízení provedeného Plnění.
- 1.3. **Akceptační řízení** je postupné provedení akceptačních procesů a podepsání Akceptačního/ch protokolu/ů pro Plnění dle Smlouvy.
- 1.4. **Aktualizace** je dílčí změna verze Softwaru, zpravidla odstraňující zranitelnosti či drobné nedostatky Softwaru většinou neprojevující se navenek uživatelům, v IT obvykle označovaná jako „patch“ nebo „security update“ (v rámci IT se také často označuje jako změna třetí číslice v čísle verze Softwaru, tedy např. 4.1.1. na 4.1.2.). Aktualizace představuje takovou změnu Softwaru, která není Modernizací ani Zásadní modernizací.
- 1.5. **Autorské dílo** znamená dílo ve smyslu § 2 Autorského zákona; zejména nikoliv však výlučně Software, Databáze a jakékoliv výstupy předávané Objednateli na základě Smlouvy, které splňují podmínky stanovené v § 2 Autorského zákona.
- 1.6. **Autorský zákon** znamená zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
- 1.7. **Čas nahlášení Incidentu** představuje časový údaj, vyjadřující datum a čas, kdy byl Incident nahlášen Dodavateli způsobem stanoveným ve Smlouvě, tj. vytvořením ticketu v Helpdesku, vytěžením e-mailu z e-mailového serveru Objednatele a jeho vložení do Helpdesku jako ticketu anebo ukončením telefonátu.
- 1.8. **Data** jsou jakékoliv údaje či informace vznikající v souvislosti s Plněním dle Smlouvy.
- 1.9. **Databáze** znamená databázi splňující požadavky na Autorská díla, databázi ve smyslu § 88 Autorského zákona a jakoukoliv jinou Autorským zákonem neupravenou databázi.
- 1.10. **Doba vyřešení** je pro každou kategorii Incidentů uvedena ve Smlouvě a znamená rozdíl mezi časem nahlášení Incidentu a dodáním řešení. Do Doby vyřešení Incidentu se nezapočítává doba, po kterou nemůže Dodavatel řešit Incident z důvodu:
 - a. neobdržení podkladů a informací vyžádaných Dodavatelem, které jsou nezbytně nutné pro lokalizaci nebo replikaci Incidentu, od Objednatele;
 - b. řešení Incidentu u třetí osoby (vyjma Poddodavatele), jejíž součinnost je dle Smlouvy povinen zajistit Objednatel (např. poskytovatele služeb podpory IT prostředím Objednatele anebo systémů, na které je Software napojen);
 - c. neposkytnutí jiné nezbytně nutné součinnosti Objednatele vyžádané Dodavatelem v souladu s těmito ZOP či Smlouvou a souvisejícími přílohami.
- 1.11. **Doba zahájení řešení incidentu (RTI)** je Doba, která uplyne od času nahlášení Incidentu Ohlašovatelem prostřednictvím Helpdesku a okamžikem předání řešení Incidentu na skupinu řešitelů.
- 1.12. **Dodavatel** označuje rovněž Poskytovatele, Zhotovitele či Prodávajícího v závislosti na typu uzavřené Smlouvy.
- 1.13. **Dokumentace** znamená část specifikace Předmětu Smlouvy, která představuje jednotlivé dokumenty popisující Předmět Smlouvy a zacházení s ním, jako jsou uživatelská dokumentace, administrátorská dokumentace, bezpečnostní dokumentace, a také jakoukoliv jinou dokumentaci vytvářenou anebo poskytovanou Dodavatelem v rámci provádění Plnění. Dokumentace musí být vždy vyhotovena a předána Objednateli v elektronické podobě (pokud je vyhotovována v listinné podobě, pak Dodavatel předá Objednateli elektronickou kopii takové Dokumentace).

- 1.14. **Dostupnost** znamená stav Softwaru, v průběhu kterého je, anebo by v případě poskytování řádné a včasné součinnosti ze strany Objednatele za podmínek dle Smlouvy byl možný řádný provoz Softwaru v celém jeho rozsahu nebo jeho podstatné části, přičemž Software se považuje za Dostupný, je-li přístupný a použitelný pro všechny uživatele Softwaru.
- 1.15. **Důvěrné informace** znamenají informace, které jsou zpracovávány, ukládány nebo poskytovány v IT prostředí Objednatele, včetně Dat Objednatele, veškeré údaje a informace související s těmito informacemi, s technickým vybavením, komunikačními prostředky a programovým vybavením IT prostředí Objednatele a s objekty, ve kterých jsou tyto systémy umístěny, zaměstnanci nebo dodavateli podílejícími se na provozu, rozvoji, správě nebo bezpečnosti IT prostředí Objednatele. Mezi Důvěrné informace nepatří informace, které jsou veřejně přístupné.
- 1.16. **FOSS licence** znamená Free Open Source Software licence.
- 1.17. **GDPR** znamená nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
- 1.18. **GUI** znamená grafické uživatelské rozhraní.
- 1.19. **Hardware** znamená veškeré hmotné součásti počítačových systémů a veškeré související vybavení hmotné povahy spolu se vším příslušenstvím, a včetně veškeré související dokumentace.
- 1.20. **Informační či komunikační systém** znamená informační či komunikační systém kritické informační infrastruktury Objednatele ve smyslu § 2 b) ZKB nebo jiný informační či komunikační systém, na který se vztahuje ZKB.
- 1.21. **Incident** představuje neplánované přerušení fungování Předmětu Smlouvy, jakékoliv jeho části anebo Plnění dle Smlouvy, omezení kvality fungování Předmětu Smlouvy a souvisejícího Plnění, anebo jakoukoliv prokazatelnou nefunkčnost Předmětu Smlouvy a souvisejícího Plnění. Incident se projevuje zejména selháním oproti funkčnosti a funkcionalitě specifikované v Příloze Smlouvy *Specifikace Plnění*, anebo obvyklé pro Předmět Smlouvy. Vada je vždy Incidentem a jde tak o podmnožinu pojmu Incident. Za dobu trvání Incidentu se považuje doba od Času nahlášení Incidentu Ohlašovatelem do vyřešení Incidentu, které bude Ohlašovatelem nebo jeho nadřízeným uživatelem potvrzeno vhodným způsobem v Helpdesku, byl-li Incident vyřešen.
- Kategorizace Incidentů dle důležitosti, zohledňující naléhavost a dopad Incidentu:
- A) Vysoká – ohrožení kritických procesů a činností na straně Objednatele
 - B) Střední – Zásadní vliv na důležité procesy a činnosti Objednatele
 - C) Nízká – standardní řešení v efektivním režimu
- 1.22. **Instalace** znamená provedení veškerých činností nezbytných ke zprovoznění Hardwaru nebo Softwaru vč. jeho Aktualizací, Modernizací či Zásadních modernizací poskytnutých v rámci Plnění dle Smlouvy v IT prostředí Objednatele, a to na platformě určené Objednatelem.
- 1.23. **ISDS** znamená informační systém datových schránek ve smyslu zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.
- 1.24. **Interní předpisy** znamenají interní předpisy Objednatele, jejichž seznam včetně znění daných interních předpisů, jsou-li relevantní z hlediska Plnění, je uveden v Příloze Smlouvy *Seznam interních předpisů*.
- 1.25. **Insolvenční zákon** znamená zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.
- 1.26. **IT prostředí Objednatele** znamená veškerý Hardware ve vlastnictví Objednatele a Software, ve vztahu k němuž je Objednatel nositelem potřebných oprávnění, nebo Hardware a Software využívaný Objednatelem na základě jiného právního titulu než Smlouvy. Jedná se zejména o servery, diskové pole a stanice, aplikace třetích osob, pasivní a aktivní datová infrastruktura (kabeláže, switche, VPN linky apod.). Podrobná specifikace IT prostředí Objednatele je uvedena v Příloze Smlouvy *Platforma Správy železnic* a v Příloze Smlouvy *Specifikace Plnění*.
- 1.27. **Kvalifikovaná osoba** je člen Realizačního týmu, kterým Dodavatel prokazoval splnění kvalifikačních předpokladů v rámci Veřejné zakázky.

- 1.28. **Kybernetický bezpečnostní incident** je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací podle § 7 ZKB v důsledku Kybernetické bezpečnostní události.
- 1.29. **Kybernetická bezpečnostní událost** je událost podle § 7 ZKB, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
- 1.30. **Modernizace** je změna verze Softwaru, která zpravidla představuje výraznější zásah do dílčí funkcionality Softwaru, přepracováním jeho vybrané funkcionality či doplnění funkcionality nové, zvýšení kompatibility Softwaru s jinými prvky informačních a komunikačních technologií, či jinou optimalizací funkce Softwaru nad rámec Aktualizace, zpravidla v IT označovaná jako „update“ (v rámci IT se také často označuje jako změna druhé číslice v čísle verze Softwaru, tedy např. 4.1. na 4.2.).
- 1.31. **NÚKIB** znamená Národní úřad pro kybernetickou a informační bezpečnost.
- 1.32. **Občanský zákoník** znamená zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
- 1.33. **Obchodní podmínky** znamenají obchodní podmínky Objednatele v posledním znění ke dni podání nabídky do Veřejné zakázky či aktualizace těchto Obchodních podmínek provedené v souladu se Smlouvou po dobu jejího trvání.
- 1.34. **Objednatel** je Správa železnic, státní organizace, IČO 70994234, se sídlem Praha 1 – Nové Město, Dlážděná 1003/7, PSČ 110 00, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. Zn. A 48384.
- 1.35. **Ohlašovatel** znamená uživatel Předmětu Smlouvy; případně osoba určená Objednatelem dle vymezení parametrů Helpdesku
- a. pro úroveň L1 Helpdesku uživatele Softwaru;
 - b. pro úroveň L2 Helpdesku osoby určené Objednatelem dle jeho potřeb zajišťující úroveň L1 podpory;
 - c. pro úroveň L3 Helpdesku člen Realizačního týmu určený Dodavatelem dle jeho potřeby zajišťující úroveň L2 podpory.
- 1.36. **Opční právo** představuje vyhrazenou změnu závazku v souladu s ustanovením § 100 odst. 3 ZZVZ ze Smlouvy spočívající v pořízení dalšího obdobného Plnění od vybraného uchazeče v rámci zadávacího řízení Veřejné zakázky, tj. od Dodavatele dle Smlouvy.
- 1.37. **Osobní údaje** znamenají osobní údaje ve smyslu GDPR, včetně zvláštních kategorií osobních údajů ve smyslu článku 9 a rozsudků ve smyslu článku 10 GDPR.
- 1.38. **Pracovní den (PD)** znamená kterýkoliv den, kromě soboty a neděle a dnů, na něž připadá státní svátek nebo ostatní svátek podle platných a účinných právních předpisů České republiky.
- 1.39. **Plnění** představuje plnění, které tvoří Předmět Smlouvy a k němuž se váže povinnost Dodavatele toto plnění Objednateli poskytovat. Plnění je blíže specifikované ve Smlouvě a v Příloze Smlouvy *Specifikace Plnění*.
- 1.40. **Poddodavatel** znamená kteroukoli třetí osobu realizující poddodávky pro Dodavatele v souvislosti s Předmětem Smlouvy. Poddodavatelé mohou být výslovně uvedeni v Příloze Smlouvy *Poddodavatelé*.
- 1.41. **Požadavek** znamená žádost ze strany Objednatele o službu nebo její podporu předanou v souladu se Smlouvou Dodavateli, která nemá příčinu v chybovém stavu, tj. není Incidentem.
- Kategorizace Požadavků dle důležitosti:
- A) Vysoká – řešení je pro Objednatele kritické
 - B) Střední – řešení neovlivňuje využívání hlavních funkcí služby
 - C) Nízká – řešení výrazně neovlivňuje procesy Objednatele
- 1.42. **Produkční prostředí** znamená IT prostředí Objednatele v ostrém provozu běžně přípustnou uživatelům Software, vyjma Testovacího prostředí.
- 1.43. **Provozovatel** znamená provozovatel ve smyslu § 2 písm. g) ZKB.
- 1.44. **Předmět Smlouvy** znamená dle typu Smlouvy Software nebo Hardware, přičemž parametry a vlastnosti Předmětu Smlouvy jsou blíže specifikovány v Příloze Smlouvy *Specifikace Plnění*.

- 1.45. **Převzetí poskytování plnění** je předání znalostí Dodavateli a praktické seznámení se Dodavatelem s podmínkami poskytování služeb. Pokud dochází k převzetí poskytování podpory, jsou podmínky pro Převzetí poskytování plnění uvedeny ve Smlouvě a v Příloze Smlouvy *Specifikace Plnění*.
- 1.46. **Příloha Smlouvy** je dokument, který tvoří nedílnou součást Smlouvy a obsahuje bližší specifikaci smluvních podmínek.
- 1.47. **Reakce** znamená kvalifikovanou a konkrétní odpověď na nahlášení Incidentu nebo na jiný požadavek, ve formě a způsobem dále definovanými v Příloze Smlouvy *Specifikace Plnění*.
- 1.48. **Reakční doba** je pro každou kategorii Incidentů uvedena v Příloze *Specifikace Plnění* a představuje dobu od Času nahlášení Incidentu do doručení Reakce Objednateli nebo Ohlašovatelí.
- 1.49. **Realizační tým** znamená osoby uvedené v příloze Smlouvy *Realizační tým*, kterými Dodavatel prokazoval splnění kvalifikačních předpokladů v rámci Veřejné zakázky a další osoby (zaměstnanci Dodavatele či Poddodavatele), prostřednictvím nichž Dodavatel provádí Plnění dle Smlouvy.
- 1.50. **Recovery Point Objective (RPO)** je parametr, který vyjadřuje maximální ztrátu dat uživatelů při havárii systému a následné obnově.
- 1.51. **Recovery Time Objective (RTO)** je parametr, který vyjadřuje dobu nutnou k obnově chodu služby do akceptované úrovně provozu.
- 1.52. **Helpdesk** je Software provozovaný Dodavatelem nebo Objednatelem sloužící ke komunikaci Stran v průběhu provádění Plnění dle Smlouvy, v rámci něhož bude evidován postup Dodavatele při provádění Plnění dle Smlouvy a zároveň bude sloužit jako kontaktní místo Dodavatele pro nahlašování požadavků, otázek, odpovědí a další zaznamenávání průběhu provádění Plnění dle Smlouvy.
- 1.53. **Servisní model** je standardizovaný model provozu a podpory aplikace, systému nebo instance služby.
- 1.54. **SLA** znamená úroveň kvality Plnění představující dohodu o úrovni poskytovaných ICT služeb dle Smlouvy.
- 1.55. **Software** znamená veškeré programové vybavení a další Autorská díla, stejně jako další věci či jiné majetkové hodnoty, které s programovým vybavením souvisí a jsou určeny ke společnému užívání s tímto programovým vybavením, tj. zejména Databáze, GUI, zvukové nahrávky, videa, obrázky, fotografie apod., včetně veškeré související dokumentace a updatů a upgradů tohoto programového vybavení, avšak s výjimkou Hardwaru a Databází.
- 1.56. **Standardní Software** znamená software, který je distribuován pod standardními licenčními podmínkami více třetím osobám. Mezi Standardní software patří:
- a. Software renomovaných výrobců, jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň dvěma (2) na sobě nezávislými a vzájemně se neovládajícími subjekty, a který je v době uzavření Smlouvy prokazatelně užíván v produkčním prostředí nejméně u pěti (5) na sobě nezávislých a vzájemně nepropojených subjektů.
 - b. Software, u kterého je s ohledem na jeho (i) marginální význam, (ii) nekomplikovanou propojitelnost či (iii) oddělitelnost a nahraditelnost v IT prostředí bez nutnosti vynakládání větších prostředků (více než 50.000 Kč/rok) zajištěno, že další rozvoj Softwaru jinou osobou než tvůrcem/distributorem takového Softwaru je možné provádět bez toho, aby tím byla dotčena práva autorů takového Softwaru, neboť nebude nutné zasahovat do Zdrojových kódů takového Softwaru anebo proto, že případné nahrazení takového Softwaru nebude představovat výraznější komplikaci a náklad na straně Objednatele.
 - c. Software, jehož API („Application Programming Interface“) pokrývá všechny moduly a funkcionality Softwaru, je dobře dokumentované, umožňuje zapouzdření Softwaru a jeho adaptaci v rámci měnících se podmínek IT prostředí Objednatele a Softwaru bez nutnosti zásahu do Zdrojových kódů Softwaru, a Dodavatel poskytne Objednateli právo užít toto rozhraní pro programování aplikací ve stejném rozsahu jako Software.
 - d. Software, o kterém to stanoví Smlouva.
- 1.57. **Smlouva** uzavřená na základě zadávacího řízení Veřejné zakázky vztahující se k ICT, která se řídí těmito ZOP.

- 1.58. **Testy** se rozumí provádění testovacího užívání Předmětu Smlouvy v Testovacím prostředí prostřednictvím simulace ostrého provozu v Produkčním prostředí a reálných situací a Testovacích scénářů.
- 1.59. **Testovací prostředí** znamená virtuální či fyzickou kopii Předmětu Smlouvy anebo IT prostředí Objednatele určenou Objednatelem k provádění Testů.
- 1.60. **Vada kategorie A** znamená kritickou vadu, která má zásadní dopad na základní funkce Plnění, má jakýkoli vliv na kvalitu a bezpečnost dat a výsledky jejich zpracování anebo způsobuje výpadky Plnění.
- 1.61. **Vada kategorie B** znamená vadu umožňující provoz základních funkcí Plnění, zároveň nemá vliv na kvalitu ani na bezpečnost dat a výsledky zpracování anebo hrozí, že by mohla způsobit výpadek Plnění.
- 1.62. **Vada kategorie C** znamená vadu, která není Vadou kategorie A anebo B (např. špatná grafická úprava aplikace, špatný pravopis u nápovědy apod.).
- 1.63. **Veřejná zakázka** je zakázka realizovaná na základě smlouvy mezi Objednatelem a Dodavatelem, jež byla uzavřena na základě zadávacího řízení dle ZZVZ nebo výběrového řízení dle vnitřních předpisů Objednatele.
- 1.64. **VKB** znamená vyhlášku č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.
- 1.65. **Výkaz** znamená dokument obsahující souhrnnou evidenci poskytnutého Plnění za období vymezené ve Smlouvě nebo v Příloze Smlouvy *Specifikace Plnění*. Výkaz je vystavován zpětně za vymezené období.
- 1.66. **Výpadek** znamená neplánované přerušení provozu Předmětu smlouvy či jakékoliv jeho podstatné části, při kterém je tento celek či příslušná část nedostupná pro uživatele (není dostupný). Za Výpadek se pro účely této Smlouvy nepovažuje Výpadek způsobený z důvodů způsobených třetími osobami, jejichž součinnost anebo bezvadné poskytování služeb je povinen zajistit Objednatel (poskytovatel služeb podpory IT prostředí Objednatele a informačních systémů, na které je Software napojen).
- 1.67. **Újma** znamená vždy újmu na jmění (škodu) ve smyslu § 2894 odst. 1 Občanského zákoníku a dále vždy i nemajetkovou újmu ve smyslu § 2894 odst. 2 Občanského zákoníku. Toto ustanovení je výslovným ujednáním o povinnosti stran odčinit nemajetkovou újmu v případech porušení povinností dle těchto ZOP a Smlouvy.
- 1.68. **Významný dodavatel** znamená Dodavatel, který je Provozovatelem, jakož i každý, kdo s Objednatelem vstupuje do právního vztahu, který je významný z hlediska bezpečnosti Informačního či komunikačního systému ve smyslu § 2 odst. m) VKB.
- 1.69. **Významná změna** znamená změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko, např.
- a. změny pravidel ochranných systémů aplikačních firewallů a pravidel přepínání a směrování v sítích,
 - b. změny autentizačních mechanismů,
 - c. přidání, změna nebo odebrání služeb, informačních systémů/aplikací nebo ochranných systémů,
 - d. změny, které umožňují sdílení informací, služeb nebo zdrojů mimo provozní prostředí,
 - e. změny opatření pro zajištění bezpečnosti vzdáleného přístupu,
 - f. zavedení skriptů pro automatické přihlášení,
 - g. migrace dat do jiné Databáze, apod. ve smyslu § 2 odst. o) VKB.
- 1.70. **Zadávací dokumentace** je souborem dokumentů obsahujících zadávací podmínky, sdělované nebo zpřístupňované účastníkům zadávacího řízení na Veřejnou zakázku.
- 1.71. **Zásadní modernizace** je podstatná změna/roziřování funkčnosti nebo změna koncepce Softwaru, přinášející podstatné změny pro chování Softwaru vůči uživatelům, zpravidla v IT označovaná jako „upgrade“ (v rámci IT se také často označuje jako změna v čísle verze Software, tedy např. 4 na 5).
- 1.72. **Zdrojový kód** znamená zápis kódu počítačového programu (Softwaru) v programovacím jazyce, který je uložen v jednom nebo více editovatelných souborech, čitelný, opatřený komentáři vysvětlujícími jeho jednotlivé části alespoň ve standardu obvyklém pro open source projekty a procesy, ve spustitelném formátu odpovídajícím programovacímu jazyku a

Produkčnímu prostředí, včetně ověřeného a podrobného postupu nezbytného pro sestavení plně funkčního strojového kódu, a v podobě, aby jej bylo možné zkompileovat do strojového kódu bez nutnosti provedení jiných úprav než kompilace v souladu s postupem k sestavení.

- 1.73. **ZKB** znamená zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
- 1.74. **ZOP** znamená tento dokument, tedy zvláštní obchodní podmínky, které definují další parametry a upřesňují konkrétní podmínky a specifické požadavky Objednatele.
- 1.75. **ZZVZ** znamená zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.
- 1.76. Není-li výslovně uvedeno jinak nebo nevyplývá-li něco jiného z povahy věci, mají pojmy, které nejsou definovány v těchto ZOP, význam uvedený v Obchodních podmínkách či Smlouvě a jejich přílohách.
- 1.77. Ustanovení ZOP mají přednost před ustanoveními Obchodních podmínek, pokud jsou ustanovení těchto dokumentů v rozporu, uplatní se ustanovení uvedené v ZOP. Ustanovení Smlouvy mají přednost před ustanoveními Obchodních podmínek i ZOP.

2. DOBA A MÍSTO PLNĚNÍ

- 2.1. Provádění Plnění bude zahájeno ode dne nabytí účinnosti Smlouvy, není-li ve Smlouvě stanoveno jinak.
- 2.2. Plnění nebo dílčí části Plnění bude Dodavatel provádět v termínech sjednaných ve Smlouvě či definovaných v Příloze Smlouvy *Specifikace Plnění* nebo *Harmonogram*.
- 2.3. Místem provádění Plnění jsou místa umístění IT prostředí Objednatele (tj. Testovací prostředí a Produkční prostředí), není-li ve Smlouvě anebo Příloze Smlouvy *Specifikace Plnění* výslovně stanoveno jinak. Popis IT prostředí Objednatele obsahuje Příloha Smlouvy *Platforma Správy železnic*.
- 2.4. Služby budou poskytovány formou vzdáleného přístupu k IT prostředí Objednatele, není-li ve Smlouvě stanoveno jinak. Objednatel se zavazuje umožnit Dodavateli vzdálený přístup k IT prostředí Objednatele. Objednatel je oprávněn monitorovat a logovat přístupy Dodavatele do IT prostředí Objednatele, jakož i veškerou další aktivitu Dodavatele významnou z hlediska bezpečnosti Informačního či komunikačního systému za účelem posouzení souladu Plnění Smlouvy s pravidly uvedenými v těchto ZOP, zejm. pak v čl. 20. ZOP, a Dodavatel se zavazuje Objednateli za tímto účelem poskytnout veškerou nutnou součinnost. Vzdálený přístup k IT prostředí Objednatele může být Objednatelem okamžitě odepřen v případě Kybernetické bezpečnostní události ve smyslu § 7 ZKB či porušení povinností stanovených v Interních předpisech.
- 2.5. Dodavatel bere na vědomí, že přístup k IT prostředí Objednatele:
 - a. je udělován fyzickým osobám Dodavatele, jakož i pro konkrétní zařízení, na základě výslovného požadavku Dodavatele a Objednatel je oprávněn dle svého uvážení přístup neudělit či kdykoli odebrat;
 - b. je poskytován na základě principů "need to know" a "deny by default"; a
 - c. je poskytován za podmínky dodržování veškerých bezpečnostních opatření a požadavků Objednatele.

3. PRÁVA A POVINNOSTI OBOU STRAN

- 3.1. Strany se zavazují postupovat v souladu s veškerými obecně závaznými právními předpisy a prohlašují, že Smlouva je v souladu s těmito právními předpisy. Pokud se v průběhu trvání Smlouvy některé její ustanovení dostane do rozporu s kogentním ustanovením obecně závazného právního předpisu, platí příslušné ustanovení právního předpisu s tím, že zbývající ustanovení Smlouvy zůstávají v platnosti.
- 3.2. Strany jsou v průběhu Plnění povinny postupovat v souladu s Interními předpisy Objednatele, pokud jsou jednoznačně specifikovány v Příloze Smlouvy *Seznam Interních předpisů*. Podpisem Smlouvy Dodavatel prohlašuje, že měl možnost se seznámit s Interními předpisy Objednatele, jejichž seznam je uveden v Příloze Smlouvy *Seznam interních předpisů*, a dále bere na vědomí, že Interní předpisy mohou být přiměřeným způsobem jednostranně měněny či jinak doplňovány Objednatelem, přičemž každá nová verze je pro Dodavatele závazná vždy ode dne, kdy se s ní seznámil či měl prokazatelnou možnost se s nimi seznámit. Rozsah Interních předpisů může být Objednatelem jednostranně rozšířen o další dokumenty stanovující jeho interní procesy.

4. POVINNOSTI DODAVATELE

- 4.1. Dodavatel se zavazuje provádět pro Objednatele Plnění osobně, tj. prostřednictvím svých zaměstnanců, členů Realizačního týmu a prostřednictvím svých Poddodavatelů za podmínek stanovených ve Smlouvě a těchto ZOP. V případě, že je požadavek na složení Realizačního týmu uveden ve Smlouvě, je Dodavatel povinen provádět Plnění výhradně prostřednictvím členů Realizačního týmu, kterými prokázal splnění kvalifikace v průběhu zadávacího řízení na Veřejnou zakázku.
- 4.2. Dodavatel se během poskytování Plnění pro Objednatele zavazuje informovat Objednatele o Významné změně ovlivnění nebo ovládání Dodavatele podle ust. § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů (dále jen „ZOK“), nebo změně vlastnictví zásadních aktiv, využívaných Dodavatelem k Plnění Smlouvy a změně oprávnění nakládat s těmito aktivy.
- 4.3. Dodavatel se zavazuje poskytovat v rámci Plnění veškerou součinnost nezbytnou k provádění Plnění, zejména, nikoliv však výlučně:
 - a. poskytovat Plnění dle Smlouvy ve vysoké kvalitě s odbornou péčí odpovídající podmínkám sjednaným ve Smlouvě;
 - b. poskytovat Plnění dle Smlouvy alespoň v závazných parametrech kvality dle Smlouvy a SLA, a to zejména dodržování stanoveného Servisního modelu dle článku 12.2. ZOP;
 - c. upozorňovat Objednatele včas na všechny hrozící vady svého Plnění či potenciální Výpadky či jiné výpadky Plnění, jakož i poskytovat Objednateli veškeré informace, které jsou pro Plnění potřebné;
 - d. zajistit v souladu s podmínkami Smlouvy poskytnutí Dokumentace, a to rovněž vždy při každé Aktualizaci nebo jiné změně Předmětu smlouvy, nestanoví-li Objednatel jinak;
 - e. počínat si při provedení Plnění tak, aby nedošlo k infikaci Softwaru, Standardního Softwaru nebo IT prostředí Objednatele virem či jiným škodlivým kódem (malware apod.) způsobujícím narušení zabezpečení Softwaru a Standardního Softwaru za účelem jeho poškození či jiného narušení běhu;
 - f. bez zbytečného odkladu oznamovat Objednateli všechny Kybernetické bezpečnostní události a Kybernetické bezpečnostní incidenty s potenciálním negativním dopadem na Objednatele;
 - g. bez zbytečného odkladu na výzvu Objednatele předat Data, provozní údaje a informace ve formátu předem odsouhlaseném Objednatelem (zpravidla ve formátu daného prostředí, který umožňuje jejich nasazení „as is“ do prostředí), které má k dispozici v souvislosti s Plněním Smlouvy, a poskytnout Objednateli za tímto účelem veškerou nezbytnou součinnost; tato Data musí být po dobu poskytování Plnění dle Smlouvy uložena u Dodavatele a mohou být Dodavatelem užívána v souladu se Smlouvou a příslušnými právními předpisy, avšak pouze v nezbytném rozsahu. Dodavatel se zavazuje dodržovat přiměřená technická a organizační opatření k ochraně těchto Dat. Veškerá Data jsou vlastnictvím Objednatele, není-li ve Smlouvě výslovně stanoveno jinak. Toto ustanovení se uplatní obdobně i na jiná data poskytnutá Objednatelem Dodavateli;
 - h. plnit Interní předpisy Objednatele a jeho pokyny v oblasti likvidace Dat (ať už Dat na papírových médiích, Dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoli dalších nosičů Dat) a případně dále na výzvu Objednatele bez zbytečného odkladu zlikvidovat Data v souladu s těmito pravidly a pokyny. Dodavatel musí především postupovat tak, aby nebylo možné odstraněná data zneužít. Za odpovídající způsob likvidace dat je považováno odstranění, přepsání či fyzická likvidace nosiče informace v souladu se standardem US DoD 5220.22-M;
 - i. poskytnout při ukončení smluvního vztahu přiměřenou součinnost při Převzetí poskytování Plnění novým Dodavatelem nebo Objednatelem, a to s odbornou péčí, zodpovědně a do doby úplného Převzetí poskytování Plnění.

5. POVINNOSTI OBJEDNATELE

- 5.1. Objednatel je povinen zajistit Testovací a Produkční prostředí pro činnost Dodavatele v rámci IT prostředí Objednatele, pokud je to nezbytné pro provádění Plnění. Zajištění prostředí zahrnuje zajištění vzdáleného přístupu personálu Dodavatele do IT prostředí Objednatele, v přiměřeném rozsahu odpovídajícího možnostem Objednatele a Zadávací dokumentaci a při respektování bezpečnostních pravidel Objednatele, zejména bezpečnostní

dokumentace, která je součástí Interních předpisů. Objednatel je povinen zajistit fungování Dodavatelem vytvořeného Testovacího prostředí, na kterém bude Software Testován, a Produkčního prostředí, na kterém Software poběží v ostrém provozu, přičemž všechna prostředí budou umístěna na IT prostředí Objednatele, není-li ve Smlouvě stanoveno jinak.

6. LICENČNÍ UJEDNÁNÍ

6.1. Software

- 6.1.1. V případě, že je Software Autorské dílo vznikající v průběhu Plnění, Dodavatel postupuje na Objednatele oprávnění k výkonu majetkových práv autorských k takovému Autorskému dílu (ve formě strojového i Zdrojového kódu) tak, aby Objednatel byl oprávněn takové Autorské dílo užít v maximálním možném rozsahu včetně oprávnění k provádění změn a předání novému dodavateli.
- 6.1.2. Dodavatel prohlašuje, že Autorské dílo dle článku 6.1.1. ZOP bylo vytvořeno zaměstnanci či Poddodavateli jako zaměstnanecké dílo ve smyslu § 58 odst. 1 a 7 Autorského zákona, a že je oprávněn k postoupení výkonu majetkových práv v souladu s tímto článkem a má k takovému postoupení náležitě souhlasy, přičemž Dodavatel se zavazuje na požádání Objednatele neprodleně předložit nebo jinak vhodným způsobem zpřístupnit dokumenty prokazující rozsah oprávnění Dodavatele.
- 6.1.3. Objednatel je dále oprávněn postoupit oprávnění k výkonu majetkových práv na jakoukoli další třetí osobu dle volby Objednatele a udělovat licence a podlicence, s čímž Dodavatel výslovně souhlasí; pro zamezení pochybnostem je Dodavatel povinen podniknout veškeré kroky k získání náležitých oprávnění tak, aby mohl oprávnění k výkonu majetkového práva postoupit na Objednatele v souladu s tímto článkem. S povinností převodu oprávnění k výkonu majetkových práv se pojí povinnost předání Zdrojového kódu dle čl. 7 ZOP.
- 6.1.4. Dodavatel dále prohlašuje, že má svolení autora/ů k zásahům do Autorského díla dle článku 6.1.1. ZOP ve smyslu § 58 odst. 4 Autorského zákona a tato svolení se vztahují na jakékoliv třetí osoby, jež budou vykonávat autorská majetková práva k tomuto Autorskému dílu.
- 6.1.5. Dodavatel dále prohlašuje, že vyloučil oprávnění autorů dle ustanovení § 58 odst. 3 Autorského zákona i vůči všem budoucím vykonavatelům autorských majetkových práv k Autorskému dílu dle článku 6.1.1. ZOP.
- 6.1.6. Dodavatel dále převádí veškerá zvláštní práva pořizovatele k Databázím pořízeným v průběhu provádění Plnění. Nedojde-li z jakéhokoliv důvodu k převodu práva dle předchozí věty, uděluje Dodavatel Objednateli oprávnění k vytěžování a zužitkování celého obsahu takové Databáze nebo její kvalitativně nebo kvantitativně podstatné části a právo udělit jinému oprávnění k výkonu tohoto práva.
- 6.1.7. K ostatním majetkovým hodnotám, které spadají pod pojem Software a zároveň nespádají pod definici Autorského díla, uděluje Dodavatel Objednateli oprávnění v rozsahu dle článku 6.1.8. ZOP. Ustanovení článku 6.2. ZOP tímto nejsou dotčena.
- 6.1.8. Nevznikne-li Objednateli z jakéhokoliv důvodu ke kterékoliv části Softwaru oprávnění k výkonu autorských majetkových práv, uděluje Dodavatel Objednateli k dotčené části množstevně a územně neomezenou výhradní licenci ke všem známým způsobům užití, a to na dobu trvání autorských majetkových práv. Objednatel je oprávněn k dotčené části Softwaru udělovat licence, tyto dále postoupit a udělovat podlicence třetím osobám. Objednatel je oprávněn dotčené části upravovat, zpracovávat, spojovat s jinými díly a jinak zasahovat do osobnostních autorských práv. Dodavatel odpovídá za zajištění těchto souhlasů.
- 6.1.9. Dodavatel není oprávněn pro účely vývoje Softwaru použít software licencovaný pod FOSS licencemi, jejichž podmínky by stanovovaly Objednateli povinnost sdělovat nebo jinak šířit Software nebo jeho části včetně Zdrojových kódů třetím osobám, nebo umožnit jim změny, úpravy či jiné zásahy do Softwaru nebo jeho částí.
- 6.1.10. Dodavatel se zavazuje nahradit veškerou Újmu, která vznikne Objednateli v důsledku nesplnění jakýchkoliv povinností dle článku 6.1. ZOP. V případě, že jakákoliv třetí osoba bude uplatňovat vůči Objednateli jakékoliv nároky spojené se Softwarem nebo jeho částí v důsledku domnělého porušení svých autorských práv, zavazuje se Dodavatel hradit nároky, které Objednatel účelně vynaložil na ochranu zájmů Objednatele v této věci (včetně právního zastoupení), a to až do právního

vyřešení nároků třetích osob; tímto není dotčena povinnost dle první věty tohoto bodu.

6.2. Standardní Software

- 6.2.1. V případech, kdy je součástí Předmětu Smlouvy dodání Standardního Softwaru, Dodavatel poskytuje nevýhradní licenci, čímž se rozumí nevýhradní nevýlučné oprávnění Autorské dílo užít v souladu s dalšími podmínkami článku 6.2. ZOP, přičemž nevýhradní licence je poskytována Objednateli dále za následujících podmínek, není-li ve Smlouvě či v Příloze Smlouvy *Specifikace Plnění* stanoveno výslovně jinak:
- a. Nevýhradní oprávnění k výkonu práva užít (licenci, resp. podlicenci) Autorské dílo včetně práva užít další Autorská díla a vytěžovat a zužítkovat Databáze, jež jsou určeny ke společnému užívání se Standardním Softwarem a za tímto účelem jsou společně distribuovány, a to všemi způsoby odpovídajícími účelu, pro který jsou taková Autorská díla, resp. Databáze, určeny, a to na dobu trvání majetkových práv autorských, nebo alespoň na dobu trvání Smlouvy.
 - b. Dodavatel je povinen zajistit poskytnutí podpory (subscription/licence maintenance) Standardního Softwaru, tj. zajistit poskytování nejnovějších verzí Standardního Softwaru získaných z důvěryhodných zdrojů Objednateli a dalších služeb v souladu se standardními licenčními podmínkami Standardního Softwaru, na dobu trvání majetkových práv autorských, pokud je to možné, jinak alespoň na dobu trvání Smlouvy.
 - c. Dodavatel je povinen poskytnout Objednateli o zajištění oprávnění ke Standardnímu Softwaru písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.
 - d. Oprávnění musí vždy umožňovat Objednateli používání Standardního Softwaru pro interní potřeby Objednatele a jemu podřízených složek, organizací, částí nebo s ním propojených právnických osob.
- 6.2.2. Licence se vztahuje ve stejné míře jako ke Standardnímu Softwaru na:
- a. Aktualizaci, Modernizaci a Zásadní modernizaci;
 - b. Dokumentaci specifikovanou v Příloze Smlouvy *Specifikace Plnění*;
 - c. Dokumentaci nad rámec Dokumentace dle předchozího bodu;
 - d. právo zužítkovat a vytěžovat Databáze, pokud jde o jiné Databáze než dle Smlouvy; a pokud tyto souvisí a jsou vhodné či nezbytné k naplnění účelu a Předmětu Smlouvy;
 - e. loga či jiné předměty duševního vlastnictví, které se Standardním Softwarem souvisí a jsou vhodné či nezbytné k užití spolu se Standardním Softwarem.
- 6.2.3. Je-li Standardní Software nebo Dokumentace vytvářena, upravována anebo jinak modifikována pro potřeby Objednatele, je Objednateli v takovém případě udělována licence k takto pro Objednatele vytvořeným či modifikovaným částem Standardního Softwaru nebo Dokumentace, včetně práva dané části jakkoliv měnit, udělit podlicenci nebo licenci zcela či z části postoupit a použít takové části Standardního Softwaru či Dokumentace k jakémukoliv účelu, v jakémkoliv množství, na jakémkoliv území, jakýmkoliv způsobem a na dobu trvání majetkových práv autorských, a to vše i prostřednictvím třetí osoby.
- 6.2.4. Pokud se jedná o Standardní Software a Dodavatel není oprávněn udělit alespoň nevýhradní licenci, pak se Dodavatel zavazuje udělit či zajistit udělení nevýhradního oprávnění k výkonu práva užít (licenci, resp. podlicenci) veškerá Autorská díla a k výkonu práva vytěžovat a zužítkovat Databáze, a to všemi způsoby odpovídajícími účelu, pro který je takové Autorské dílo, resp. Databáze, určeno, a to alespoň na dobu trvání Smlouvy. Dodavatel je povinen zajistit poskytnutí podpory Standardního Softwaru dle tohoto článku, tj. zajistit poskytování nejnovějších verzí Standardního Softwaru Objednateli získaných z důvěryhodných zdrojů a dalších služeb v souladu s jeho standardními licenčními podmínkami, na dobu trvání Smlouvy. Dodavatel je povinen poskytnout Objednateli písemné prohlášení o zajištění oprávnění ke Standardnímu Softwaru a na výzvu Objednatele tuto skutečnost prokázat. Oprávnění dle tohoto článku musí vždy umožňovat Objednateli používání Standardního Softwaru pro interní potřeby Objednatele a jemu podřízených složek, organizací, částí nebo s ním propojených právnických osob.

- 6.2.5. V ostatních parametrech se udělení licence řídí licenčními podmínkami výrobce Standardního Softwaru.
- 6.2.6. Ustanovení čl. 6.1. ZOP a 6.3. ZOP a jeho podčlánků se pro Standardní Software nepoužijí.
- 6.3. Software vztahující se k Hardwaru
 - 6.3.1. V případech, kdy je k řádnému užívání dodaného Hardwaru potřebný určitý Software, je Dodavatel povinen poskytnout/zajistit Objednateli jako součást Plnění a za cenu zahrnutou v ceně Hardwaru, oprávnění užít tento Software v rozsahu, způsoby a za účelem obvyklým ve vztahu k Hardwaru, se kterým je spojen, nejméně však za podmínek dle Přílohy Smlouvy Specifikace Plnění.
 - 6.3.2. Ustanovení čl. 6.1. ZOP a jeho podčlánků a 6.2. ZOP a jeho podčlánků se pro Software vztahující se k Hardwaru nepoužijí.
- 6.4. Odměna za poskytnutí oprávnění dle článku 6. ZOP je zahrnuta v Ceně za Plnění dle Smlouvy.

7. ZDROJOVÝ KÓD A DOKUMENTACE

- 7.1. Zdrojový kód bude předáván Objednateli na datovém nosiči vždy na konci Akceptačního řízení, nebo za podmínek stanovených ve Smlouvě, zejména pokud bude smluvní vztah ukončen bez provedení Akceptačního řízení.
- 7.2. Na datovém nosiči dat musí být viditelně označen „Zdrojový kód“ s označením části Modifikace a jeho verze a den předání Zdrojového kódu. O předání nosiče dat bude oběma Smluvními stranami sepsán a podepsán písemný předávací protokol.
- 7.3. Povinnost Dodavatele předávat Zdrojový kód se přiměřeně použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update Zdrojového kódu v rámci následného provádění Plnění anebo v rámci záručních oprav. Zdrojový kód musí obsahovat podrobný popis a komentář každého zásahu do Zdrojového kódu.
- 7.4. Objednatel nebude v průběhu provádění Plnění sám anebo prostřednictvím jiných osob zasahovat do Zdrojového kódu nasazeného anebo fungujícího v Produkčním prostředí či Testovacím prostředí.
- 7.5. Dodavatel je povinen předat Objednateli příslušnou Dokumentaci a Zdrojový kód ve standardní podobě (to nejméně v kvalitě obvyklé pro open source projekty), vždy obsahující následující:
 - a. Kompletní Zdrojové kódy celého díla.
 - b. Uživatelskou příručku obsahující konkrétní popis uživatelského prostředí, funkcí a postupů pro zaškolení zaměstnanců.
 - c. Administrátorskou příručku, popisující všechny parametry, které lze konfigurovat a popis dopadů změny konfigurace do systému.
 - d. Technickou dokumentaci systému, pakliže se jedná o vícevrstvou architekturu, popis každé vrstvy zvlášť:
 - (i) Datová vrstva – popis datové vrstvy, čili tabulek v databázi včetně vazeb mezi tabulkami a včetně E-R schémat.
 - (ii) Aplikační vrstva – popis jádra systému, jeho funkcí, služeb a rozhraní. Dokumentace musí obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.
 - (iii) Prezentační vrstva – Dokumentace systému musí obsahovat drátové modely všech obrazovek uživatelského rozhraní včetně popisu funkcí prvků každé obrazovky.
 - e. Popis konfigurace provozního prostředí systému (serverová strana i klientská strana).
 - f. Dokumentace musí obsahovat soupis všech požadavků na nastavení hardwarových a softwarových komponent běhového prostředí jako jsou:
 - (i) mapování souborových systémů;
 - (ii) požadavky na operační paměť a procesory;

- (iii) konfigurační parametry jednotlivých podpůrných Softwarových prostředků (např. specifika pro nastavení databáze, aplikačního serveru, webového serveru apod.).
 - g. Objednatel požaduje, aby tato Dokumentace byla ve formátech XML DocBook (zdrojové) a PDF (export z XML zdroje pro snadnou distribuci uživatelům) nebo případně v jiném formátu, který Objednatel schválí po vzájemné dohodě s Dodavatelem. Všechny Dokumentace musí být verzované, opatřené seznamem autorů, přehledem změn jednotlivých verzí a musí být obsahově úplné pro tu část systému, kterou popisují.
 - h. Řešení musí obsahovat návod na používání systému (uživatelský manuál) a popis systému – jeho vlastností, strukturu projektu, použité technologie (technická dokumentace). Součástí řešení je i Dokumentace a automaticky generovaná dokumentace (Javadoc). Součástí Dokumentace musí být zip archiv se zdrojovými soubory řešení a programátorskou dokumentací.
- 7.6. V případě jakýchkoli pochybností o správnosti předání Zdrojového kódu se bude uvedené posuzovat podle svého účelu, tedy zejména následné možnosti provádět samostatně či prostřednictvím třetích osob opravy, změny, doplnění, uprady nebo updaty Zdrojového kódu. Za nesprávné předání se přitom považuje takové předání, které v důsledku vede ke znemožnění či podstatnému ztížení práce se Zdrojovým kódem ve výše uvedeném smyslu.

8. AKCEPTAČNÍ ŘÍZENÍ

- 8.1. Předání a převzetí Předmětu Smlouvy, včetně předání a převzetí výstupů provádění Plnění, dokumentů majících charakter výstupů Předmětu Plnění a Zdrojových kódů, probíhá na základě Akceptačního řízení, tj. postupným provedením akceptačních procesů a podepsáním Akceptačního/ch protokolu/ů.
- 8.2. Akceptační řízení zahrnuje porovnání skutečných vlastností Provádění Plnění se specifikací Plnění dle Smlouvy a Akceptačními kritérii. Podrobnější rozsah Akceptačních kritérií je součástí Přílohy Smlouvy *Specifikace Plnění*.
- 8.3. Plnění dle Smlouvy a jakékoliv jeho části, které podléhají Akceptačnímu řízení, jsou provedeny skončením Akceptačního řízení dotčené části Plnění, v případě Plnění jako celku skončením Akceptačního řízení Plnění jako celku.
- 8.4. Na Akceptační řízení se uplatní následující pravidla:
- a. Dodavatel je povinen písemně informovat Objednatele nejméně čtrnáct (14) dní předem o termínu předání výstupu k Akceptačnímu řízení, nedohodnou-li se Strany jinak;
 - b. Dodavatel předá Objednateli výstup provádění Plnění k realizaci Akceptačního řízení; Akceptační řízení může být zahájeno pouze v případě, že výstup provádění Plnění, který je předmětem takového Akceptačního řízení, je umístěn v Produkčním anebo Testovacím prostředí nebo byl jiným způsobem Dodavatelem skutečně předán Objednateli a ten se s ním mohl seznámit; Objednatel na žádost Dodavatele potvrdí převzetí výstupů k Akceptačnímu řízení v Helpdesku, e-mailem, anebo prostřednictvím ISDS; převzetím k Akceptačnímu řízení anebo potvrzením ve smyslu tohoto článku je zahájeno Akceptační řízení;
 - c. po provedení všech nezbytných činností v rámci Akceptačního řízení se Objednatel i Dodavatel zavazují podepsat příslušný protokol potvrzující provedení výstupu provádění Plnění anebo výsledek Testů výstupů provádění Plnění připravený Dodavatelem a upravený a vyplněný Objednatelem (Akceptační protokol). Akceptační protokol obsahuje:
 - (i) Specifikaci provedeného Plnění;
 - (ii) Akceptační kritéria;
 - (iii) informace o průběhu Testů, jsou-li prováděny;
 - (iv) další informace a dokumenty nezbytné pro provedení Akceptačního řízení provedeného Plnění nebo jeho části.
 - d. v případě nutnosti opakování činností v rámci Akceptačního řízení v důsledku uvedení výroku „Neakceptováno“ v Akceptačním protokolu Dodavatel Objednateli opět předá výstup k opětovnému provedení činností v rámci Akceptačního řízení (další kolo

- Akceptačního řízení) a Dodavatel připraví nový Akceptační protokol vztahující se k dalšímu kolu Akceptačního řízení;
- e. je-li součástí Plnění několik výstupů, pak každý z takových výstupů podléhá samostatnému Akceptačnímu řízení;
 - f. Akceptační řízení konkrétního výstupu končí a výstup se považuje za provedený podpisem Akceptačního protokolu Objednatelem s uvedeným výrokem „Akceptováno“ nebo odstraněním vytčených vad výstupu v případě vyznačení „Akceptováno s výhradou“ a potvrzením odstranění takových vytčených vad Objednatelem na Akceptačním protokolu, který obsahoval vytčené vady.
- 8.5. Objednatel je povinen po provedení ověření kvality výstupu v rámci Akceptačního řízení Dodavateli podepsat Akceptační protokol a akceptovat výstup provádění Plnění, případně oznámit Dodavateli vady výstupu provádění Plnění, které brání jeho provedení včetně určení Kategorie vady A, B, C.
- 8.6. Výstupy provádění Plnění jsou způsobilé k akceptaci Objednatelem, pokud:
- a. naplňují Akceptační kritéria a nevykazují žádné vady, pak Objednatel vyznačí na Akceptačním protokolu „Akceptováno“; nebo
 - b. naplňují Akceptační kritéria a vykazují vady, které nebrání tomu, aby výstup provádění Plnění sloužil svému účelu bez významnějších omezení pro Objednatele (zejména organizačních, časových, nákladových apod.), anebo v případě Softwaru při Testech či provozu v souhrnu nevykazují více vad, než připouští Akceptační kritéria, pak Objednatel vyznačí na Akceptačním protokolu „Akceptováno s výhradou“.
- V jiných případech vyznačí Objednatel na Akceptačním protokolu „Neakceptováno“.
- 8.7. V případě splnění Akceptačních kritérií je Objednatel povinen do 30 dnů od zahájení Akceptačního řízení vyznačit na Akceptačním protokolu výrok „Akceptováno“. V případě nesplnění Akceptačních kritérií Objednatel vyznačí do 30 dnů od zahájení Akceptačního řízení na Akceptačním protokolu výrok „Neakceptováno“ a uvede všechna Akceptační kritéria, která považuje za nesplněná s uvedením, v čem spočívá jejich nesplnění. Objednatel není povinen výše uvedené lhůty dodržet, dojde-li k prodloužení Akceptačního řízení z důvodu na straně Dodavatele.
- 8.8. Pokud Objednatel akceptuje výstup provádění Plnění svým podpisem a vyznačením výroku „Akceptováno s výhradou“, které na Akceptačním protokolu uvede společně s uvedením vad, které nebrání akceptaci, zavazuje se Dodavatel k odstranění těchto vad ve lhůtách výslovně stanovených v Akceptačním protokolu, a pokud nejsou takové, pak lhůtách přiměřených stanovených Objednatelem v rámci odstraňování vad vyznačených v Akceptačním protokolu s výrokem „Akceptováno s výhradou“ postupují Strany dle předchozích ustanovení tohoto článku až do odstranění všech vad vyznačených v Akceptačním protokolu s výrokem „Akceptováno s výhradou“.
- 8.9. V případě neschválení výstupu provádění Plnění vyznačením na Akceptačním protokolu „Neakceptováno“ odstraní Dodavatel vady uvedené v Akceptačním protokolu ve lhůtách výslovně stanovených v Akceptačním protokolu Objednatelem, a pokud nejsou takové, pak lhůtách přiměřených. Do odstranění vad bránících akceptování je výstup provádění Plnění považován za neakceptovaný (neprovedený). Po odstranění vad uvedených v Akceptačním protokolu Dodavatel předá znovu výstup provádění Plnění Objednateli k dalšímu kolu Akceptačního řízení a Objednatel postupuje obdobně podle předchozích ustanovení tohoto článku a specifických podmínek Akceptačního řízení uvedených v tomto článku.
- 8.10. Akceptační řízení se užije i na akceptaci a schválení výkazů či reportů, je-li jejich pravidelné zasílání Objednateli součástí Plnění.
- Akceptační řízení však bude v takovém případě probíhat pouze následovně:
- a. výkaz a report, včetně všech jeho součástí, se považuje za akceptovaný doručení Dodavateli sdělení Objednatele, že Objednatel jej považuje za úplný a správný, a souhlasí s vystavenou fakturou; nebo
 - b. marným uplynutím lhůty pro posouzení úplnosti a správnosti faktury, která se týká stejného období jako výkaz a report, bez vznesení připomínek ze strany Objednatele.

9. ŠKOLENÍ

- 9.1. Dodavatel provede zaškolení příslušných zaměstnanců Objednatele pro Software nebo Hardware v termínu dle Smlouvy, a pokud takový termín není, pak v termínu určeném Objednatelem po dohodě s Dodavatelem.

- 9.2. Součástí školení je i poskytnutí Dokumentace pro provedení školení a komplexní administraci Softwaru nebo užívání Hardwaru tak, aby na základě Dokumentace byli účastníci absolvující školení schopni samostatně (bez zásahů Dodavatele) ovládat Software nebo Hardware.
- 9.3. Účelem provedení školení je seznámení účastníků školení se Softwarem nebo Zařízením do té míry, aby jej byli schopni samostatně užívat v souladu se svým pracovním zařízením u Objednatele.
- 9.4. Požadavek na školení bude stanoven ve Smlouvě. Pokud Smlouva či její Příloha obsahuje požadavek na provedení školení, provede Dodavatel seznámení zaměstnanců Objednatele s Předmětem Smlouvy za podmínek, jež jsou uvedeny v tomto článku.
- 9.5. Dodavatel je dále povinen provést v přiměřeném rozsahu školení příslušných zaměstnanců Dodavatele a dalších osob podílejících se na poskytování Plnění dle Smlouvy za účelem splnění povinností dle čl. 20. ZOP. Tuto skutečnost je povinen na vyžádání Objednateli prokázat.

10. HELPDESK

- 10.1. Dodavatel se zavazuje:
 - 10.1.1. nejpozději do dne účinnosti Smlouvy založit a po celou dobu trvání Smlouvy udržovat v provozu Helpdesk (včetně úhrady případných licenčních poplatků za aplikaci Helpdesk) a udělit náležitá oprávnění k přístupu do Helpdesku Ohlašovatelům a dalším pověřeným uživatelům dle pokynů Objednatele, včetně Objednatelem určeného počtu přístupů. Helpdesk bude fungovat prostřednictvím webové adresy, elektronické pošty nebo telefonního čísla;
nebo
 - 10.1.2. po celou dobu trvání Smlouvy užívat Helpdesk provozovaný Objednatelem.
- 10.2. Provozovatele Helpdesku stanoví Smlouva. Pokud Smlouva provozovatele Helpdesku nestanoví, má se za to, že provozovatelem Helpdesku je Dodavatel. V případě, že provozovatelem bude Objednatel, poskytne Dodavateli nezbytnou součinnost k řádnému užívání Helpdesku včetně případného poskytnutí licencí.
- 10.3. Dodavatel se zavazuje zajistit Helpdesk v jednom z následujících režimů, který je vymezen ve Smlouvě:
 - a. **Režim 1:**
7x24, tj. dvacet čtyři (24) hodin sedm (7) dní v týdnu prostřednictvím přímého přístupu do Helpdesku na webové adrese určené Dodavatelem/Objednatelem dle provozních podmínek aplikace Helpdesk, případně prostřednictvím přímého datového propojení Helpdesků Objednatele a Dodavatele.
 - b. **Režim 2:**
7x24, tj. dvacet čtyři (24) hodin sedm (7) dní v týdnu prostřednictvím elektronické pošty na adrese určené Dodavatelem.
 - c. **Režim 3:**
5x8, tj. v Pracovních dnech v době od 9:00 do 17:00 na telefonním čísle určeném Dodavatelem.
- 10.4. Helpdesk v režimu 1 dle článku 10.3. ZOP zahrnuje mimo jiné příjem a evidenci Požadavků, oznámení o potřebě součinnosti Objednatele a dalších zpráv, potvrzování jejich přijetí, předávání jednotlivých úkolů odpovědným osobám, sledování stavu, průběhu a procesu prací a dalších zpráv, informování o stavu řešení, vytváření přehledů a statistik, a to přes přehledné webové rozhraní. Je-li Helpdesk provozován Dodavatelem musí být zabezpečen tak, aby odpovídal požadavkům vyplývajícím ze ZKB a Interních předpisů. Výstupem z Helpdesku je záznam o veškerých úkonech Helpdesku ve formě přehledného logu, jež umožňuje vyhledávání a uchovávání záznamů tak, aby byly naplněny požadavky ZKB a Interních předpisů na takové záznamy.
- 10.5. Helpdesk bude dostupný pouze pro Objednatele a Ohlašovatele.
- 10.6. Helpdesk je provozován v některé z těchto úrovní podpory, která je vymezena ve Smlouvě:
 - a. první úroveň (L1) – nahlášení Incidentu Ohlašovatelem je prováděno nahlášením Objednateli či pověřené osobě Objednatele, který Incident vyhodnotí a případně předá Incident jako Incident Dodavateli do druhé úrovně podpory;

- b. druhá úroveň (L2) – nahlášení Incidentu Ohlašovatelem Dodavateli v případě, že Incident nebyl vyřešen v první úrovni podpory – je prováděno nahlášením Ohlašovatelem přes Helpdesk Dodavateli;
 - c. třetí úroveň (L3) – nahlášení Incidentu eskalační úrovni podpory Dodavatele nebo nahlášení Dodavatelem třetí osobě, která je oprávněna anebo schopna vyřešit Incident, pokud nebyl vyřešen v druhé úrovni podpory – je prováděno nahlášením Ohlašovatelem přes Helpdesk eskalační úrovni Dodavatele anebo Dodavatelem třetí osobě.
- 10.7. Ohlašovatelem s přístupem do Helpdesku
- a. je pro úroveň L1 Helpdesku uživatel Softwaru nebo Hardwaru;
 - b. jsou pro úroveň L2 Helpdesku osoby určené Objednatelem dle jeho potřeb zajišťující úroveň L1 podpory;
 - c. je pro úroveň L3 Helpdesku člen Realizačního týmu určeného Dodavatelem dle jeho potřeby zajišťující úroveň L2 podpory.

11. NAHLÁŠENÍ INCIDENTU

- 11.1. Hlášení o Incidentu Dodavateli bude provedeno Ohlašovatelem, a to přímým zadáním Incidentu do Helpdesku, odesláním e-mailu nebo telefonátem na kontaktní číslo Helpdesk, přičemž Ohlašovatel je povinen uvést popis Incidentu, a to v následujícím rozsahu:
- a. krátký a rámcově výstižný název Incidentu;
 - b. identifikace části Předmětu Plnění, které se Incident týká;
 - c. určení prostředí (Testovací prostředí, Produkční prostředí);
 - d. detailní popis Incidentu, průvodních jevů a všech významných souvisejících informací;
 - e. kategorii Incidentu (A, B, C);
 - f. identifikaci Ohlašovatele.
- 11.2. V případě, že některá z náležitostí dle čl. 11.1. ZOP chybí nebo je nedostatečná, může si Dodavatel vyžádat její doplnění od Ohlašovatele; tato skutečnost však nemá vliv na určení Času nahlášení Incidentu, ledaže bez tohoto doplnění hlášení Incidentu postrádá informaci natolik podstatnou, že bez ní objektivně nelze přistoupit k řešení Incidentu.
- 11.3. Je-li Incident nahlašován zadáním Incidentu do Helpdesku, pak se za Čas nahlášení Incidentu považuje čas vytvoření ticketu v Helpdesku. Je-li Incident nahlašován písemně na e-mailovou adresu, pak se za Čas nahlášení Incidentu považuje čas odeslání e-mailu z e-mailového serveru Ohlašovatele, nebo v případě hlášení Incidentu telefonicky čas ukončení telefonického hovoru. Dodavatel je povinen prokazatelným způsobem bezodkladně potvrdit přijetí nahlášení Incidentu, a to vždy prostřednictvím Helpdesku. Nepotvrdí-li Dodavatel přijetí Incidentu, nemá to vliv na Čas nahlášení Incidentu.
- 11.4. Dodavatel se zavazuje po dobu poskytování Plnění evidovat všechny nahlášené Incidenty a způsob jejich řešení, včetně časových údajů o průběhu řešení jednotlivých Incidentů ve Výkazech.
- 11.5. Není-li v Servisní smlouvě, jejích přílohách anebo Technické specifikaci stanoveno jinak, ustanovení článku 11. ZOP se použijí přiměřeně i na nahlášení a evidování Požadavků; v takovém případě se za Čas nahlášení Incidentu považuje Čas nahlášení Požadavku.

12. SERVISNÍ MODEL

- 12.1. Servisní model představuje standardizovaný model provozu a podpory aplikace, systému nebo instance služby.
- 12.2. Pokud je součástí Smlouvy zajištění provozu a podpory Softwaru nebo Hardwaru, je ve Smlouvě vymezen jeden z níže uvedených Servisních modelů:

Servisní model	Dostupnost	Doba provozu	Doba zpracování Incidentu		Doba řešení Incidentů kategorie A	Doba řešení Incidentů kategorie B	RTO	RPO	Doba zpracování Požadavku	Doba řešení Požadavku kategorie A	Doba řešení Požadavku kategorie B
A1 Kritický	99.5%	7x24	(0-24)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A2 Kritický	99.5%	7x12	(6-18)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A3 Kritický	99.5%	5x8	(7-15)	1 hod	2 hod	2 hod	4 hod	< 5 min	1 PD	1 PD	3 PD
A4 Kritický	99.5%	7x24	(0-24)	1 hod	4 hod	12 hod	4 hod	< 5 min	1 PD	2 PD	5 PD
A5 Kritický	99.5%	5x8	(7-15)	1 hod	4 hod	12 hod	4 hod	< 5 min	1 PD	2 PD	5 PD
B1 Závažný	98.0%	7x24	(0-24)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD
B2 Závažný	98.0%	7x12	(6-18)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD
B3 Závažný	98.0%	5x8	(7-15)	1 PD	2 PD	3 PD	48 hod	30 min	2 PD	3 PD	5 PD
C1 Normální	97.0%	5x12	(6-18)	1 PD	3 PD	6 PD	96 hod	24 hod	3 PD	7 PD	10 PD
C2 Normální	97.0%	5x8	(7-15)	1 PD	3 PD	6 PD	96 hod	24 hod	3 PD	7 PD	10 PD
D Minoritní	94.0%	5x8	(7-15)	2 PD	10 PD	14 PD	96 hod	24 hod	5 PD	10 PD	14 PD
E1 Customizovaný											
E2 Customizovaný											

12.3. Doba řešení Incidentu a Požadavku kategorie C je pro veškeré Servisní modely stanovena na 15 PD.

12.4. Do měření úrovně Dostupnosti nejsou započítávány:

- dočasné vyřazení Softwaru z provozu na základě předchozí dohody Objednatele a Dodavatele (odstávka),
- pravidelná vyřazení Softwaru z provozu Dodavatelem v časech sjednaných ve Smlouvě nebo její příloze (servisní okna),
- smluvními stranami předem dohodnutý časový úsek za účelem instalace upgradu,
- výpadky Softwaru způsobené Objednatelem přímo v důsledku jím provedených zásahů do Softwaru, které nebyly Dodavatelem předem schváleny,

12.5. Nedostupnost Softwaru dle článku 0. ZOP se nepovažuje za nedosažení sjednaných parametrů Dostupnosti dle Smlouvy a nebude započítána do výpočtu dle článku 12.6. a 12.7. ZOP.

12.6. Nestanoví-li Smlouva jinak, bude Dostupnost Software měřena na základě následujícího vzorce:

$$\text{Dostupnost (\%)} = \frac{\text{Doba provozu} - \text{Doba výpadku}}{\text{Doba provozu}} \times 100$$

12.7. Doba výpadku Softwaru je časový úsek z Doby provozu v hodinách, kdy je služba nedostupná, a počítá se podle následujícího vzorce:

$$\text{Doba výpadku} = \sum_i^n T_i$$

kde:

Σ je celková doba všech výpadků Softwaru za vyhodnocované období

T_i je doba jednotlivého výpadku Softwaru

- 12.8. Doba Provozu Softwaru definovaná pro účely tohoto článku je celková doba provozu Softwaru v hodinách za vyhodnocované období, kterým je kalendářní měsíc.

13. ÚČAST PODDODAVATELŮ

- 13.1. Poddodavatele, jejichž prostřednictvím Dodavatel prokazoval kvalifikaci ve Veřejné zakázce, je Dodavatel povinen využívat při Plnění Smlouvy po celou dobu jejího trvání v rozsahu, v jakém jimi prokazoval kvalifikaci. Poddodavatele, jimiž Dodavatel prokazoval kvalifikaci ve Veřejné zakázce, lze vyměnit pouze s předchozím listinným souhlasem Objednatele, který může být dán výlučně za předpokladu, že tyto osoby budou nahrazeny osobami splňujícími kvalifikaci požadovanou ve Veřejné zakázce ve stejném rozsahu jako nahrazované osoby.
- 13.2. Dodavatel se zavazuje, že při poskytování Plnění pro Objednatele budou všichni Poddodavatelé, které Dodavatel využívá k poskytnutí Plnění dle Smlouvy, dodržovat veškeré požadavky vyplývající ze Smlouvy a Příloh Smlouvy. Dodavatel odpovídá za to, že jeho Poddodavatelé nebudou jednat v rozporu s ujednáními Smlouvy a jejími Přílohami, kterou mezi sebou uzavřeli Dodavatel a Objednatel.
- 13.3. Významný dodavatel je oprávněn využit k Plnění dle Smlouvy Poddodavatele neuvedené ve Smlouvě jen v případě, že to Smlouva výslovně připouští, a to za podmínek v ní uvedených. Nestanoví-li Smlouva jinak, podléhají jednotliví Poddodavatelé Významného dodavatele předchozímu písemnému schválení ze strany Objednatele. Dodavatel může ke schválení navrhnout nebo do Plnění Smlouvy zapojit pouze takové Poddodavatele, kteří nejsou v rozporu s požadavky Objednatele na Významného dodavatele.

14. REALIZAČNÍ TÝM

- 14.1. Pokud je takový požadavek součástí Zadávací dokumentace, je Dodavatel povinen předat Objednateli seznam osob, které budou členy Realizačního týmu, který se bude podílet na Plnění dle Smlouvy. Členy Realizačního týmu lze měnit pouze s předchozím listinným souhlasem Objednatele, který může být dán výlučně za předpokladu, že tyto osoby budou nahrazeny osobami splňujícími kvalifikaci požadovanou ve Veřejné zakázce ve stejném rozsahu jako nahrazované osoby. Při změně Realizačního týmu není nutné uzavírat listinný dodatek ke Smlouvě a Dodavatel je povinen vypracovat a předat Objednateli v listinné podobě aktualizované znění seznamu členů Realizačního týmu. Tento článek se týká pouze Veřejných zakázek, které požadují provádění Plnění prostřednictvím Realizačního týmu.
- 14.2. Dodavatel se zavazuje provádět Plnění prostřednictvím členů Realizačního týmu uvedených v Příloze Smlouvy *Realizační tým* tak, aby jednotliví členové Realizačního týmu, kteří jsou Kvalifikovanými osobami, prováděli činnosti na pozici dle jejich odbornosti (kvalifikace), které odpovídají tomu, pro jakou pozici prokazovali kvalifikaci v rámci Veřejné zakázky, a v rozsahu, který takové pozici běžně odpovídá.
- 14.3. Každá Kvalifikovaná osoba musí po celou dobu provádění Plnění splňovat kvalifikaci uvedenou v nabídce Dodavatele a zároveň minimální technické kvalifikační předpoklady kladené na pozici, kterou daná osoba zastává dle Zadávací dokumentace.
- 14.4. Nebude-li se Kvalifikovaná osoba řádně podílet na provádění Plnění v rozsahu stanoveném Smlouvou, např. v důsledku ukončení její spolupráce s Dodavatelem nebo její dlouhodobé absence (zejména dlouhodobá nemoc pravděpodobně překračující délku jednoho měsíce), je Dodavatel povinen neprodleně namísto Kvalifikované osoby zahájit provádění Plnění Náhradní Kvalifikovanou osobou a nejpozději do tří (3) Pracovních dnů ode dne, kdy taková situace nastala, informovat Objednatele o této skutečnosti.
- 14.5. Pokud Objednatel nesouhlasí s osobou Náhradní Kvalifikované osoby, je oprávněn žádat Dodavatele o její výměnu za jinou osobu se stejnou kvalifikací navrženou Dodavatelem, čemuž je Dodavatel povinen vyhovět.

15. KOMUNIKACE STRAN

- 15.1. Objednatel a Dodavatel si pro vzájemnou komunikaci ohledně Smlouvy zvolí kontaktní osoby, jejichž seznam uvedou ve Smlouvě.
- 15.2. Jsou-li naplněny podmínky článku 20.1. ZOP, vykonává kontaktní osoba na straně Dodavatele povinnosti kontaktní osoby pro kybernetickou bezpečnost vyplývající z článku 20. ZOP, nebo je pro plnění takových povinností Dodavatel povinen určit zvláštní kontaktní osobu ve Smlouvě (v takovém případě obě Strany zvolí kontaktní osobu pro kybernetickou bezpečnost, která má na starosti komunikaci týkající se článku 20. ZOP).

- 15.3. Strany si navzájem oznámí jakékoliv změny v kontaktních osobách, přičemž taková změna je účinná uplynutím sedmého (7.) dne po jejím doručení.
- 15.4. Není-li ve Smlouvě výslovně stanovena jiná forma pro doručování dokumentů anebo jiných právních jednání, lze takové dokumenty a jednání doručit v elektronické formě na e-mailovou adresu příslušné kontaktní osoby, prostřednictvím datové zprávy zaslané v rámci ISDS, anebo v listinné podobě.

16. SMLUVNÍ POKUTY

- 16.1. Poruší-li Dodavatel některou ze svých povinností stanovených v Příloze Smlouvy *Specifikace Plnění*, zejména pak pokud poruší SLA, resp. stanovený servisní model dle článku 12.2. ZOP, je Objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši stanovené v článku 16.2. ZOP, pokud nejsou ve Smlouvě výslovně zakotveny jiné sankce, které vylučují aplikaci článku 16.2. ZOP.
- 16.2. Objednateli vzniká vůči Dodavateli právo na zaplacení smluvní pokuty:
- poruší-li Dodavatel svoji povinnost řádně a včas provést Plnění ve výši 0,01 % z celkové ceny Plnění (dále jen „Cena“) za každý započatý den prodlení až do řádného splnění této povinnosti;
 - poruší-li Dodavatel svoji povinnost řádně a včas provést jakoukoliv část Plnění ve výši 0,02 % z ceny takové části Plnění za každý započatý den prodlení až do řádného splnění této povinnosti; v případě, že by smluvní pokuty dle čl. 16.2. písm. a. a čl. 16.2. písm. b. ZOP měly běžet vůči Dodavateli zároveň, vzniká za takové období Objednateli nárok pouze dle čl. 16.2. písm. a.
 - poruší-li Dodavatel povinnost udělit nebo zajistit Objednateli ze strany třetí osoby/třetích osob udělovaná oprávnění v rozsahu práv duševního vlastnictví ve výši 5 % z Ceny za každé jednotlivé porušení;
 - poruší-li Dodavatel povinnost řádně a včas předat Objednateli Zdrojový kód a veškerou související Dokumentaci, ve výši 0,05 % z Ceny za každý započatý den prodlení;
 - poruší-li Dodavatel některou z povinností týkající se účasti Poddodavatelů anebo Realizačního týmu, ve výši 2 % z Ceny za každé jednotlivé porušení povinnosti;
 - poruší-li Dodavatel svoji povinnost dodržet sjednanou Dobu vyřešení Incidentu, ve výši:
 - ve výši 0,003 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie A;
 - ve výši 0,003 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie B;
 - ve výši 0,001 % z Ceny v případě každé započaté hodiny/den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu kategorie C;
 - v případě prodlení nad rámec sjednané lhůty pro odstranění vad v Produkčním prostředí:
 - Vada kategorie A ve výši 0,003 % z Ceny za každou započatou hodinu/den v případě každé Vady;
 - Vada kategorie B ve výši 0,003 % z Ceny za každou započatou hodinu/den v případě každé Vady;
 - Vada kategorie C ve výši 0,001 % z Ceny za každou započatou hodinu/den v případě každé Vady;
 - V případě, že Dodavatel nedodrží Dostupnost stanovenou servisním modelem dle článku 12. ZOP, ve výši dle tabulky uvedené níže v závislosti na míře nedodržení požadované Dostupnosti:

Výše poklesu Dostupnosti oproti stanovené Dostupnosti servisním modelem je	Výše smluvní pokuty
Do 2 %	3 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle čl. 12.8 ZOP

2 do 5 %	5 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle čl. 12.8 ZOP
5 do 10 %	8 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle čl. 12.8 ZOP
10 % a více	16 % z ceny poskytovaného Plnění odpovídající vyhodnocovanému období dle čl. 12.8 ZOP

- i. v případě prodlení Dodavatele reagovat na Požadavek Objednatele v době řešení incidentu uvedené v článku 12.2. ZOP ve výši z 0,007 z % Ceny za každý jednotlivý případ;
 - j. ve výši a za podmínek dle článku 20 ZOP v oblasti kybernetické bezpečnosti;
 - k. ve výši a za podmínek dle článku 21 ZOP v oblasti ochrany osobních údajů;
 - l. ve výši a za podmínek dle článku 22 ZOP v oblasti ochrany důvěrných informací; nebo
 - m. poruší-li Dodavatel svoji povinnost dle čl. 13.2 ZOP nebo 13.3. ZOP, ve výši 2 % z Ceny za každé jednotlivé porušení.
- 16.3. Pro smluvní pokuty stanovené v čl. 16.2. písm. f. a g. ZOP platí, že je-li lhůta pro splnění stanovena v hodinách, je smluvní pokuta počítána za každou započatou hodinu, je-li lhůta pro splnění stanovena ve dnech či pracovních dnech, je smluvní pokuta počítána za každý započatý den.
- 16.4. Zaplacením smluvních pokut není dotčeno právo Objednatele na náhradu újmy v plném rozsahu.
- 16.5. Smluvní pokuta je splatná do 30 dnů ode dne doručení písemné výzvy Objednatele k jejímu uhrazení. Objednatel je oprávněn započíst nárok na zaplacení smluvní pokuty, i pokud ještě není splatný, proti jakémukoliv nároku Dodavatele na peněžité plnění vyplývajícímu ze Smlouvy.
- 16.6. Za každý den prodlení s úhradou Smluvní pokuty je Objednatel oprávněn požadovat po Dodavateli úhradu úroků z prodlení ve výši stanovené obecně závaznými právními předpisy.

17. ZÁRUKA ZA JAKOST A PRÁVA Z VADNÉHO PLNĚNÍ

- 17.1. Společná ustanovení
- 17.1.1. Dodavatel uděluje Objednateli záruku za jakost Plnění a všech jeho částí na dobu dvou (2) let ode dne akceptace výstupu Plnění.
 - 17.1.2. Objednatel je oprávněn Vady, které se vyskytnou v průběhu záruční doby, nahlásit Zhotoviteli bez zbytečného odkladu od okamžiku, kdy je zjistil. Lhůta bez zbytečného odkladu činí vždy nejméně devadesát (90) dnů.
 - 17.1.3. Dodavatel odpovídá za vady zjevné, skryté i právní, které měl výstup provádění Plnění v době akceptace Objednatelem, a dále za ty, které se na něm vyskytnou v záruční době, a zavazuje se, vedle dalších nároků Objednatele, je bezplatně odstranit.
 - 17.1.4. Dodavatel neodpovídá za vady, pokud byly způsobeny zásahem do takových výstupů Plnění ze strany Objednatele nebo jím pověřené osoby, případně jiných dodavatelů Objednatele.
 - 17.1.5. Objednatel je povinen oznámit vady Plnění Dodavateli prostřednictvím Helpdesku, nebude-li Stranami dohodnuto jinak.
 - 17.1.6. Dodavatel neodpovídá za vady Plnění vzniklé:
 - a. provozováním Díla Objednatelem v rozporu s Dokumentací;
 - b. neoprávněným nebo neodborným zásahem či nesprávným užitím Díla Objednatelem;
 - c. vadami IT prostředí Objednatele.
- 17.2. Záruka vztahující se k Softwaru

- 17.2.1. Pokud výrobce Standardního Software poskytuje záruku za jakost, pak Dodavatel postupuje takovou záruku za jakost Objednateli. To nezbavuje Dodavatele povinnosti poskytnout Objednateli vlastní záruku za jakost ve smyslu tohoto článku.
- 17.2.2. V době trvání záruční doby je Dodavatel povinen odstraňovat vady ve lhůtách uvedených v tabulce níže. Lhůty stanovené v hodinách běží pouze v Pracovní dny osm (8) hodin denně v době od 9:00 do 17:00 hodin (režim 5x8). Lhůty stanovené v hodinách se mimo dobu uvedenou v předchozí větě staví a pokračují dále v běhu během další bezprostředně následující doby počítání. Strany pro zamezení pochybnostem prohlašují, že toto se netýká lhůt stanovených v Pracovních dnech ani počítání doby prodlení v rámci výpočtu smluvních pokut.

Produkční prostředí

Kategorie vady	Lhůta k odstranění počítaná od nahlášení vady Objednatel
Vada kategorie A – kritická	do 4 hodin ¹
Vada kategorie B – střední	do 17:00 třetího Pracovního dne od nahlášení vady ²
Vada kategorie C – nízká	do 17:00 pátého Pracovního dne od nahlášení vady ³

Testovací prostředí

Kategorie vady	Lhůta k odstranění počítaná od nahlášení vady Objednatel
Vada kategorie A – kritická	do 17:00 druhého Pracovního dne od nahlášení vady ⁴
Vada kategorie B – střední	do 17:00 pátého Pracovního dne od nahlášení vady ⁵
Vada kategorie C – nízká	do 17:00 desátého Pracovního dne od nahlášení vady ⁶

17.3. Záruka vztahující se k Hardwaru

- 17.3.1. Poskytuje-li výrobce anebo Dodavatel kterékoliv části Hardwaru na své výrobky anebo služby záruku za jakost delší, než je záruka za jakost dle tohoto článku, zavazuje se Dodavatel udělit Objednateli nebo na Objednatele postoupit danou záruku za jakost tak, aby Objednatel byl oprávněn po skončení záruky za jakost uplatnit nároky ze záruky za jakost bez nutnosti součinnosti ze strany Dodavatele.
- 17.3.2. Zjevné vady Hardware a dalších hmotných věcí je Objednatel povinen u Dodavatele reklamovat v rámci Akceptačního řízení. V případě, že Objednatel zjistí vady hmotných věcí po akceptaci, je povinen tyto vady bez zbytečného odkladu reklamovat u Dodavatele.
- 17.3.3. V případě, že odstranění reklamovaných vad bude trvat déle než dva (2) Pracovní dny, zavazuje se Dodavatel poskytnout Objednateli náhradní Hardware či jinou náhradní hmotnou věc po dobu trvání odstranění reklamované vady, nedohodnou-li se Strany jinak.

18. UKONČENÍ SMLUVNÍHO VZTAHU

18.1. Obecně k odstoupení od Smlouvy:

- Strany sjednávají, že vznikne-li Objednateli nárok na odstoupení od Smlouvy, může podle své volby odstoupit od Smlouvy v celém rozsahu či jen od některé části Plnění určené Objednatel.
- Strany se dohodly na vyloučení použití § 1978 odst. 2 Občanského zákoníku, který stanoví, že marné uplynutí dodatečně lhůty stanovené k plnění může mít za následek odstoupení od této Smlouvy bez dalšího.

¹ Lhůta je stanovena v hodinách.

² Lhůta je stanovena ve dnech.

³ Lhůta je stanovena ve dnech.

⁴ Lhůta je stanovena v hodinách.

⁵ Lhůta je stanovena ve dnech.

⁶ Lhůta je stanovena ve dnech.

- c. Dodavatel nemá právo odstoupit od Smlouvy v případě nevhodných příkazů Objednatele či poskytnutí nevhodné věci Objednatelem dle § 2595 Občanského zákoníku.
- 18.2. Objednatel je oprávněn odstoupit od Smlouvy, v případě, že:
- a. Dodavatel je v prodlení s plněním dle Smlouvy či jakékoliv části Plnění déle než 30 dnů a nezjedná nápravu ani do 15 dnů od doručení písemného oznámení Objednatele o takovém prodlení.
 - b. Dodavatel je v prodlení s Plněním dle Smlouvy déle než 60 dnů, a to i bez nutnosti zaslání předchozího upozornění.
 - c. Nastane některý ze zákonem stanovených případů a zejména v případech podstatného porušení povinností Dodavatele stanovených ve Smlouvě. Za podstatné porušení povinností Dodavatele se považuje zejména:
 - (i) Dodavatel je opakovaně v prodlení s prováděním Plnění dle Smlouvy;
 - (ii) prohlášení Dodavatele učiněné na základě Smlouvy se ukáže jako nepravdivé;
 - (iii) Dodavatel bez upozornění a relevantního odůvodnění nepoužil k Plnění člena Realizačního týmu, ač k tomu byl povinen; nebo
 - (iv) Dodavatel poruší některou z povinností uvedenou v čl. 20. ZOP opakovaně nebo závažným způsobem.
 - d. Dodavatel poruší kteroukoliv svoji povinnost dle Smlouvy jiným než podstatným způsobem a ve lhůtě 15 dnů od doručení písemného oznámení Objednatele toto své porušení nenapraví.
 - e. Dodavatel poruší svou povinnost dle čl. 13.2. ZOP nebo čl. 13.3. ZOP nebo Poddodavatel Dodavatele poruší některou z povinností vyplývajících z požadavků dle čl. 13.2. ZOP.
 - f. Dodavatel podá insolvenční návrh jako dlužník ve smyslu § 98 Insolvenčního zákona nebo insolvenční soud nerozhodne o insolvenčním návrhu na Dodavatele do šesti (6) měsíců od zahájení insolvenčního řízení, nebo insolvenční soud vydá rozhodnutí o úpadku Dodavatele ve smyslu § 136 Insolvenčního zákona.
 - g. Je přijato rozhodnutí o povinném nebo dobrovolném zrušení Dodavatele (vyjma případů sloučení nebo splynutí).
 - h. Okolnost vylučující povinnost k náhradě Újmy kterékoli ze Stran trvá déle než 30 dnů;
 - i. dojde k Významné změně dle čl. 4.2. ZOP.
 - j. Dojde k Významné změně kontroly nad Dodavatelem nebo změny kontroly nad zásadními aktivy využívanými Dodavatelem k plnění Smlouvy, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle ust. § 71 a násl. ZOK, či ekvivalentní postavení.
 - k. Dojde k Významné změně ovlivnění nebo ovládání Dodavatele podle ust. § 71 a násl. ZOK nebo změně vlastnictví zásadních aktiv, využívaných Dodavatelem k plnění Smlouvy a změně oprávnění nakládat s těmito aktivy, či dojde ke změně ekvivalentní těmto změnám a tato změna bude Objednatelem vyhodnocena jako riziko bezpečnosti informací, které nelze odstranit jiným opatřením; toto ustanovení se uplatní i pro případ, že Dodavatel o takových změnách dopředu a včas neinformuje Objednatele.
- 18.3. Dodavatel je oprávněn odstoupit od Smlouvy pouze v případech jejího podstatného porušení, jestliže:
- a. Objednatel nezaplatil jakoukoli dlužnou částku za Plnění dle Smlouvy řádně a včas a toto porušení nenapravil ani do 60 dnů ode dne obdržení písemné výzvy k nápravě; nebo
 - b. Objednatel poruší jinou povinnost dle Smlouvy podstatným způsobem a ve lhůtě 60 dnů ode dne obdržení písemné výzvy k nápravě toto své porušení nenapraví.
- 18.4. Dodavatel není oprávněn odstoupit od Smlouvy ve vztahu k části Plnění, za kterou mu již bylo Objednatelem zapláceno.

19. ZMĚNY SMLOUVY A ZMĚNOVÉ ŘÍZENÍ

- 19.1. Není-li ve Smlouvě nebo jejích Přílohách stanoveno jinak, může být Smlouva měněna nebo zrušena pouze v listinné podobě, a to v případě změn Smlouvy číslovanými dodatky, který musí být podepsány oběma Stranami a uzavřeny v souladu se ZZVZ.

- 19.2. Pokud je ve Smlouvě upraveno Opční právo, vyhrazuje si Objednatel v souladu s ustanovením § 100 odst. 3 ZZVZ vyhrazenou změnu závazku z této Smlouvy spočívající v pořízení dalšího obdobného Plnění od vybraného účastníka v rámci zadávacího řízení Veřejné zakázky, tj. od Dodavatele dle Smlouvy. Předmětem plnění Opčního práva je poskytnutí dalšího obdobného Plnění dle Smlouvy tak, jak bylo podrobně vymezeno včetně dalších zákonných náležitostí vyhrazené změny závazku dle § 100 odst. 3 ZZVZ v Zadávací dokumentaci předmětné Veřejné zakázky.
- 19.3. Objednatel je oprávněn do uplynutí tří (3) let od nabytí účinnosti Smlouvy kdykoliv uplatnit toto Opční právo, a to i opakovaně do vyčerpání limitů Opčního práva definovaných v Zadávací dokumentaci. Vyhrazená změna závazku ze Smlouvy bude Stranami projednána v rámci jednacího řízení bez uveřejnění dle § 66 ZZVZ, které bude zahájeno Objednatelem v souladu s tímto ustanovením, a jehož výsledkem bude uzavření listinného dodatku k této Smlouvě či uzavření nové smlouvy mezi Objednatelem nebo Dodavatelem.

20. KYBERNETICKÁ BEZPEČNOST

- 20.1. Tento článek se uplatní v případě, kdy tak výslovně stanoví Smlouva, pokud je Předmětem Smlouvy Informační či komunikační systém, pokud má Plnění dopad na Informační či komunikační systém, nebo pokud je Smlouva uzavřena s Významným dodavatelem či Provozovatelem. Zda je Dodavatel Významným dodavatelem či Provozovatelem, stanoví Smlouva. Na jiné Smlouvy a vztahy se neuplatní, ledaže se Dodavatel stane Významným dodavatelem či Provozovatelem v průběhu plnění Smlouvy. V takovém případě se na něj čl. 20. uplatní v rozsahu v jakém to po něm lze spravedlivě požadovat.
- 20.2. Dodavatel se při plnění Smlouvy zavazuje postupovat v souladu se ZKB, VKB a souvisejícími právními předpisy, dodržovat zásady bezpečnosti informací, Interní předpisy Objednatele a z nich vyplývající povinnosti týkající se bezpečnostních opatření, provozní řády prostor Objednatele, rozhodnutí, opatření obecné povahy, či jiný správní akt NÚKIB či jiného správního orgánu nebo závazné podmínky pro Objednatele stanovené orgánem veřejné moci ukládající Objednateli další povinnosti ve smyslu ZKB a VKB, včetně upozorňování a zajištění hlášení Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů Objednateli, jakož i další bezpečnostní politiky, metodiky a postupy, se kterými byl Objednatelem seznámen.
- 20.3. Dodavatel je povinen seznámit se s bezpečnostními požadavky Objednatele uvedenými ve Smlouvě, jejích přílohách, těchto ZOP, Interních předpisech Objednatele a seznámit s nimi osoby podílející se na plnění Smlouvy dle potřeby s ohledem na charakter jejich plnění s přihlédnutím k zajištění bezpečnosti informací. Kontaktní osoba Dodavatele je povinna splnění povinnosti dle předchozí věty Objednateli potvrdit do 30 dnů od uzavření Smlouvy. Pokud je to potřebné, je Dodavatel povinen provést školení bezpečnostních požadavků dle tohoto odstavce a dále je provádět v pravidelných intervalech, nejméně 1x ročně. Dodavatel je také povinen aktivně vynucovat dodržování takových bezpečnostních požadavků dotčenými osobami na straně Dodavatele. Za porušení těchto pravidel osobami uvedenými v tomto odstavci odpovídá Dodavatel tak, jako by je porušil sám.
- 20.4. Není-li ve Smlouvě ujednáno jinak, je Dodavatel povinen vytvořit, pravidelně aktualizovat a vynucovat vůči osobám podílejícím se, byť i nepřímo, na Předmětu Smlouvy:
- politikou řízení přístupu, na základě které přidělí oprávnění k výkonu činností jednotlivým rolím svých fyzických osob (přístup pro více osob na jednom účtu je nežádoucí a lze pouze se souhlasem Objednatele) podílejících se na plnění Smlouvy (zaměstnanci, programátoři podnikatelé apod.) v nejmenším možném a nutném rozsahu tak, aby měly přístup k aktivům Objednatele pouze ty osoby, které takový přístup skutečně potřebují k výkonu činností týkajících se předmětu Plnění dle Smlouvy; není-li ve Smlouvě ujednáno jinak, je Dodavatel dále povinen průběžně monitorovat a zaznamenávat přístupy všech osob účastnících se na Plnění dle Smlouvy, a to v rozsahu, aby bylo možné jednoznačně určit uživatele, čas a provedenou činnost, jakož i vyhodnocovat oprávněnost těchto přístupů (logování přístupů) a tuto svou povinnost v politice řízení přístupu zohlednit a Dodavatel musí umožnit a poskytnout součinnost na jejich integraci do systému bezpečnostního monitoringu (SIEM), systému pro správu logů a centrální úložiště logů Objednatele;
 - politikou zvládání Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů obsahující činnosti, role, odpovědnosti a pravomoci k rychlému a účinnému zvládání Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů.

- 20.5. Kontaktní osoba Dodavatele je povinna před započítím Plnění, nejpozději však do 30 dnů od uzavření Smlouvy, určit a popsat veškerá dotčená primární i podpůrná aktiva na straně Dodavatele potřebná pro plnění Smlouvy. Dodavatel je povinen při nakládání s veškerými aktivy (dotčenými aktivy Dodavatele a Objednatele) postupovat tak, aby chránil jejich důvěrnost, dostupnost a integritu a zavést přiměřená opatření na jejich ochranu. Dodavatel je povinen řídit rizika spojená s Plněním dle Smlouvy minimálně dle standardů požadovaných normou ISO 27001 a případně dle Interních předpisů, pokud obsahují závazná pravidla pro řízení rizik. Dodavatel je povinen bez zbytečného odkladu po uzavření Smlouvy kontaktní osobu Objednatele informovat o způsobu řízení rizik a o zbytkových rizicích souvisejících s Plněním Smlouvy a následně v pravidelných intervalech informovat o změnách.
- 20.6. Dodavatel je povinen zaslat kontaktní osobě Objednatele bez zbytečného odkladu všechna hlášení o událostech, která mají charakter Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu, včetně případů porušení zabezpečení Osobních údajů, vždy bez zbytečného odkladu, nejpozději však do tří (3) hodin po jejich zjištění, a sdělit Objednateli opatření, která již provedl ve vztahu k této Kybernetické bezpečnostní události anebo Kybernetickému bezpečnostnímu incidentu, případně zvolí jinou formu dohodnutou mezi Objednatелеm a Dodavatelem určenou ke včasnému hlášení Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu a/nebo již učiněných opatření. Dodavatel je povinen veškeré Kybernetické bezpečnostní události a Kybernetické bezpečnostní incidenty zaznamenávat a po nezbytně dlouhou dobu uchovávat. Dodavatel je povinen poskytnout Objednateli veškerou nezbytnou součinnost k detekci, vyhodnocení či řešení Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu, a to včetně případné realizace nutných opatření dle pokynů Objednatele. Zapříčinil-li Dodavatel Kybernetický bezpečnostní incident nebo podílel-li se na jeho vzniku, provede analýzu příčin Kybernetického bezpečnostního incidentu a navrhne opatření za účelem zamezení jeho opakování v budoucnu. Dodavatel je povinen ohlásit každou jednotlivou Kybernetickou bezpečnostní událost nebo Kybernetický bezpečnostní incident jedním z následujících způsobů:
- a. e-mailem na adresu kontaktní osoby uvedené ve Smlouvě; nebo
 - b. telefonicky na telefonní číslo kontaktní osoby uvedené ve Smlouvě; nebo
 - c. ohlášením do Helpdesku Objednatele.
- 20.7. Dodavatel je povinen pravidelně alespoň čtvrtletně předkládat Objednateli zprávu o počtu a druhu útoků a Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů, které zaznamenal ve spojení s Plněním a/nebo Předmětem Smlouvy.
- 20.8. Dodavatel se zavazuje poskytnout Objednateli veškerou součinnost nezbytnou k tomu, aby Objednatel řádně naplňoval právní povinnosti stanovené ZKB, VKB a Interními předpisy. Zejména se Dodavatel zavazuje poskytnout Objednateli součinnost směřující k zavedení a provádění bezpečnostních opatření podle ZKB, VKB a Interních předpisů a řešení Kybernetických bezpečnostních událostí a Kybernetických bezpečnostních incidentů. Jestliže Dodavatel při plnění Smlouvy zjistí či jako odborník mohl a měl zjistit rozpor ustanovení Interních předpisů se ZKB, VKB anebo rozhodnutím či jiným pokynem NÚKIB v souladu se ZKB, je povinen takový rozpor Objednateli neprodleně ohlásit a poskytnout Objednateli součinnost k jeho odstranění.
- 20.9. Dodavatel bere na vědomí, že v rámci provádění Plnění může být podroben Interním předpisům Objednatele či jeho pokynům v oblasti řízení kontinuity činností, zejména může být zahrnut do havarijních plánů, úkolů při aktivaci řízení kontinuity činností, bezpečnostní politiky apod., a to v rozsahu, v jakém lze po Dodavateli spravedlivě požadovat s ohledem na předmět plnění.
- 20.10. V případě, že dojde k jakémukoliv rozporu mezi Dodavatelem a třetí osobou, která není jeho Poddodavatelem a je dodavatelem Softwaru nebo jiných technologií dotčených plněním povinností Dodavatele dle této Smlouvy, je Dodavatel povinen tuto skutečnost bez zbytečného odkladu oznámit Objednateli. Dodavatel je dále povinen poskytovat Objednateli nutnou součinnost pro jednání s těmito třetími osobami a sám se těchto jednání účastnit, nebo na základě žádosti Objednatele jednat s těmito třetími osobami napřímo.
- 20.11. Objednatel má právo v souladu s ustanoveními § 2593 Občanského zákoníku prostřednictvím určených osob kdykoli kontrolovat plnění Smlouvy u Dodavatele a jeho případných Poddodavatelů, a to i prostřednictvím třetí osoby; předchozí věta se uplatní obdobně v případě kontroly některé ze Stran ze strany kontrolního orgánu ve smyslu zákona č. 255/2012 Sb., kontrolní řád, ve znění pozdějších předpisů.

- 20.12. Objednatel má právo prostřednictvím určených osob provádět v pravidelných intervalech (1x ročně, není-li ve Smlouvě ujednáno jinak), jakož i v případě důvodného podezření na závažné porušení povinností Dodavatele dle těchto ZOP, v případě Kybernetických bezpečnostních incidentů a/nebo v jiných případech vyžadovaných ZKB a/nebo VKB, audit kybernetické bezpečnosti, tj. dodržování bezpečnosti informací dle Interních předpisů, ZKB a VKB u Dodavatele a jeho případných Poddodavatelů, a to i prostřednictvím třetí osoby. V rámci auditu kybernetické bezpečnosti je Objednatel oprávněn zejména porovnávat zjištěné skutečnosti s bezpečnostní dokumentací Objednatele a nad rámec obvyklý u auditu kybernetické bezpečnosti dále provádět následující činnosti:
- a. nehlášená návštěva u Dodavatele v místě umístění členů Realizačního týmu či jiných osob podílejících se na plnění Smlouvy v rozsahu tří (3) hodin vždy nejčastěji čtyřikrát (4x) za rok; a
 - b. nehlášený telefonát s členem Realizačního týmu, který má přístup do Informačního či komunikačního systému, zahrnující konkrétní dotazy na zabezpečení a jiné aspekty informační bezpečnosti dotčeného Informačního či komunikačního systému.
- 20.13. Dodavatel je povinen umožnit Objednateli provedení kontroly a auditu kybernetické bezpečnosti a zajistit (i smluvně) právo na provedení této kontroly a auditu kybernetické bezpečnosti u svých případných Poddodavatelů, jakož i veškerou další součinnost nezbytnou pro provedení auditu. Kontrolu a audit kybernetické bezpečnosti může rovněž provést i třetí osoba pověřená Objednatel. Průběh takového auditu je doložen např. auditní zprávou či jiným obdobným dokumentem. Případné náklady na straně Dodavatele na provedení auditu jsou součástí Ceny za Plnění dle Smlouvy. Dodavatel je oprávněn rozporovat výsledky auditu kybernetické bezpečnosti do 7 Pracovních dnů od oznámení výsledku auditu kybernetické bezpečnosti. Dodavatel může rozporovat a) existenci vytkénoho porušení či hrozby; b) že porušení či hrozba byla Dodavatelem již odstraněna. V obou případech uvede skutečnosti a důkazy k podpoře svých tvrzení. Objednatel je v takovém případě povinen takové připomínky vypořádat. V případě, že Objednatel na svém zjištění setrvává, je Dodavatel povinen se tímto auditem řídit.
- 20.14. Pokud audit kybernetické bezpečnosti odhalí jakékoliv podstatné porušení či hrozbu takového porušení, je Dodavatel povinen napravit nedostatky vč. přijetí případných dalších bezpečnostních opatření a o tomto informovat Objednatele, pokud se jedná o Významného dodavatele, je povinen napravit nedostatky a bezodkladně informovat Objednatele do 7 dnů.
- 20.15. Je-li součástí Předmětu Plnění přenos Dat a informací, je Dodavatel povinen jej za součinnosti oprávněných osob na straně Objednatele zabezpečit odolnými kryptografickými algoritmy v souladu s aktuálními doporučeními NÚKIB.
- 20.16. Je-li součástí Předmětu Plnění správa síťové infrastruktury a/nebo jejích prvků (aktivních či pasivních), je Dodavatel povinen za součinnosti oprávněných osob na straně Objednatele:
- a. provádět analýzy topologie sítě či skenování aktivních částí Předmětu Plnění; a
 - b. realizovat bezpečnostní opatření pro odstranění nebo blokování síťových spojení, která neodpovídají požadavkům na ochranu integrity komunikační sítě.
- 20.17. Významný dodavatel je dále povinen:
- a. poskytnout Objednateli veškeré potřebné informace a součinnost v procesu řízení a evidence změn v souladu s § 11 VKB dle potřeb Objednatele (zejm. při posouzení, zda je změna Významnou změnou, analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním, zajištění možnosti navrácení do původního stavu a provedení dalších činností dle VKB);
 - b. strpět a poskytnout Objednateli veškerou potřebnou součinnost v případě nutnosti provést penetrační testování;
 - c. zpracovat a pravidelně aktualizovat bezpečnostní dokumentaci v rozsahu stanoveném ve Smlouvě;
 - d. průběžně detekovat známé zranitelnosti dotčených aktiv Objednatele a bezodkladně na ně upozorňovat Objednatele; a
 - e. vést v elektronické formě provozní deník obsahující veškeré podstatné okolnosti související s plněním povinností Dodavatele dle článku 20. ZOP a/nebo Plněním, provozní události důležitých aktiv a relevantní záznamy o plnění povinností Dodavatele dle článku 20. ZOP a zpřístupnit jej Objednateli prostřednictvím zabezpečeného vzdáleného přístupu, není-li ve Smlouvě ujednáno jiný způsob; v provozním deníku

Významný dodavatel dále do 20. dne následujícího měsíce uvede výstup z monitoringu dostupnosti, důvěrnosti a integrity aktiv Objednatele, se kterými pracuje v rámci plnění Smlouvy, prováděného nejméně jedenkrát měsíčně a vyhodnocovaného vždy k 10. dni následujícího měsíce.

20.18. Provozovatel je dále povinen:

- a. provádět pravidelné zálohy dat a programového vybavení vztahujících se k Plnění dle Smlouvy, zabezpečit je vhodnými prostředky proti neoprávněným přístupům nebo jejich ztrátě a v pravidelných intervalech testovat funkčnost těchto záloh, nejméně jedenkrát za měsíc, není-li ve Smlouvě ujednáno jinak;
- b. plnit další povinnosti vyplývající pro Provozovatele ze ZKB a VKB.

20.19. Pokud Objednatel zjistí, že Dodavatel postupuje v rozporu s tímto článkem, je Objednatel v takovém případě oprávněn dožadovat se toho, aby Dodavatel odstranil vady vzniklé vadným postupem Dodavatele, zdržel se provádění postupů, které jsou v rozporu s tímto článkem, nebo konal, jak je od něj vyžadováno tímto článkem, a dále Smlouvou plnil řádným způsobem. Strany se dohodnou na podmínkách a lhůtě k odstranění nedostatků plnění Smlouvy ve smyslu tohoto odstavce, přičemž nedohodnou-li se Strany na konkrétní lhůtě, pak je Dodavatel povinen odstranit nedostatky do třiceti (30) dnů. Jestliže Dodavatel včas neodstraní nedostatky ve smyslu předchozí věty tohoto odstavce nebo se jedná o porušení povinnosti (bez ohledu na jeho závažnost), pak je Objednatel oprávněn od Smlouvy odstoupit.

20.20. Kontaktní osoby Stran vzájemně komunikují v průběhu plnění Smlouvy za účelem dosažení standardů pro bezpečnost informací. V případě ohrožení anebo porušení bezpečnosti informací, zejména v případě výskytu Kybernetické bezpečnostní události anebo Kybernetického bezpečnostního incidentu, jsou kontaktní osoby povinny vzájemně komunikovat, ihned po zjištění takových skutečností hlásit jejich výskyt druhé Straně a společně podnikat kroky k zajištění obnovení bezpečnosti informací.

20.21. Dodavateli nenáleží za plnění povinností souvisejících s bezpečností informací ve smyslu článku 20. ZOP jakákoliv další odměna, resp. taková odměna je součástí Ceny.

20.22. Objednatel je oprávněn požadovat na Dodavateli zaplacení smluvní pokuty:

- a. za každý den prodlení při zavedení bezpečnostních opatření podle ZKB, VKB, těchto ZOP a Interních předpisů:
 - (i) ve výši 0,05 % z Ceny po dobu prvních pěti (5) dnů prodlení;
 - (ii) ve výši 0,1 % z Ceny po dobu od šestého (6.) dne prodlení do desátého (10.) dne prodlení; a
 - (iii) ve výši 0,2 % z Ceny po dobu od jedenáctého (11.) dne prodlení;
- b. za každý den Objednatelem zjištěného soustavného porušování bezpečnostních opatření podle ZKB, VKB, těchto ZOP a Interních předpisů:
 - (i) ve výši 0,05 % z Ceny do šestého (6.) dne soustavného porušování; a
 - (ii) ve výši 0,1 % z Ceny od šestého (6.) dne soustavného porušování;
- c. ve výši 2 % z Ceny za každý případ porušení povinnosti hlášení událostí, které mají charakter Kybernetické bezpečnostní události nebo Kybernetického bezpečnostního incidentu;
- d. ve výši 2 % z Ceny za každý případ neumožnění nebo odepření provedení kontroly a auditu kybernetické bezpečnosti ve smyslu článku 20. ZOP;
- e. ve výši 5 % z Ceny za každý případ porušení článku 20. ZOP, přičemž toto porušení vedlo ke Kybernetickému bezpečnostnímu incidentu;
- f. ve výši 0,1 % z Ceny za každý započatý den trvání porušení povinností Významného dodavatele dle článku 20. ZOP, dané porušení nebylo odstraněno a negativní následek porušení povinnosti stále trvá; a
- g. ve výši 1 % z Ceny za každý případ jiného porušení článku 20. ZOP neuvedeného výše.

21. OCHRANA OSOBNÍCH ÚDAJŮ

21.1. Budou-li údaje, ke kterým Dodavatel získá přístup v souvislosti s Plněním dle Smlouvy, mít povahu Osobních údajů, je Dodavatel povinen přijmout veškerá opatření k tomu, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k těmto Osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům či jinému zneužití, a zajistit nakládání s Osobními údaji v souladu s GDPR.

- 21.2. Pokud bude v rámci provádění Plnění docházet ke zpracování Osobních údajů, je rozsah zpracovávaných Osobních údajů uveden ve Smlouvě. Pokud dojde v rámci poskytování Plnění ke zpracování Osobních údajů, které Smlouva výslovně neuvádí, budou tato nová zpracování Osobních údajů prováděna za stejných podmínek.
- 21.3. Dodavatel bude zpracovávat Osobní údaje pro Objednatele výhradně za účelem poskytování služeb v rozsahu ujednaném podle Smlouvy. Dodavatel bude pro Objednatele zpracovávat Osobní údaje výhradně za uvedeným účelem, způsobem a na základě doložených pokynů a podmínek Objednatele a v souladu s nimi tak, jak vyplývají ze Smlouvy. Dodavatel neprodleně informuje Objednatele, pokud jsou podle jeho názoru určité pokyny Objednatele v rozporu s účinnými právními předpisy.
- 21.4. Dodavatel se zavazuje přijmout vhodná technická a organizační opatření podle GDPR, které se na něj jako na zpracovatele vztahují, a plnění těchto povinností na vyžádání doložit Objednateli.
- 21.5. Dodavatel může předávat Osobní údaje do třetí země nebo mezinárodní organizaci ve smyslu GDPR pouze na základě zvláštního pokynu Objednatele. Je-li takovéto předání založeno na povinnosti vyplývající z práva Unie nebo členského státu, které se na Objednatele vztahuje, informuje Dodavatel Objednatele o tomto právním požadavku před předáním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu.
- 21.6. Dodavatel je povinen zajistit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly zachovávat mlčenlivost ve vztahu ke všem Osobním údajům, které zpracovává na základě Smlouvy, a rovněž tak o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.
- 21.7. Dodavatel je povinen přijmout všechna opatření dle čl. 32 GDPR tak, aby byla zajištěna odpovídající bezpečnost Osobních údajů. Dodavatel může do zpracování zapojit Poddodavatele pouze na základě předchozího písemného souhlasu Objednatele. Dodavatel se zavazuje s těmito Poddodavateli uzavřít smlouvu v souladu s GDPR zajišťující dodržování práv a povinností stanovených Smlouvou a/nebo těmito ZOP, zvláště pak povinnosti mlčenlivosti a zajištění bezpečnosti Osobních údajů a poskytnutí dostatečných záruk pro zavedení stejných technických a organizačních opatření Poddodavatelem, jakož i v souladu s dalšími aplikovatelnými právními předpisy. Dodavatel je dále povinen zohlednit povahu zpracování, být Objednateli nápomocen prostřednictvím vhodných technických a organizačních opatření pro splnění povinnosti Objednatele reagovat na žádost o výkon práv subjektu údajů dle GDPR.
- 21.8. Dodavatel je povinen být Objednateli nápomocen při zajišťování souladu s povinnostmi podle článku 32 až 36 GDPR, a to při zohlednění povahy zpracování informací, jež má Dodavatel k dispozici. V případech, kdy povaha věci vyžaduje informování Objednatele ze strany Dodavatele, informuje Dodavatel Objednatele bez zbytečného odkladu.
- 21.9. Dodavatel je povinen umožnit Objednateli a jím pověřené osobě během běžné pracovní doby Dodavatele provést v sídle Dodavatele kontrolu dodržování povinností týkajících se zpracování Osobních údajů vyplývajících ze Smlouvy, a to i po ukončení stanovené doby zpracování, tj. po ukončení této Smlouvy, a to do 3 měsíců od jejího ukončení.
- 21.10. Po ukončení zpracování Osobních údajů podle Smlouvy je Dodavatel povinen poskytnout Objednateli všechna Zařízení obsahující Osobní údaje, pokud je to možné, a vymazat všechny zpracovávané Osobní údaje ze všech svých systémů nebo databází, včetně vymazání všech záložních kopií, s výjimkou, kdy uchovávání vyžadují právní předpisy, nebo k tomu dal písemný souhlas Objednatel.
- 21.11. V případě, že Dodavatel zpracuje osobní údaje nad rámec vymezený Smlouvou/doloženými pokyny Objednatele, považuje se ve vztahu k takovému zpracování za správce. Pokud tímto zpracováním nad rámec vymezený Smlouvou/doloženými pokyny Objednatele vznikne Objednateli škoda, je Dodavatel povinen škodu uhradit.
- 21.12. Pokud Dodavatel poruší povinnost chránit Osobní údaje v souladu s tímto článkem, vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši částky sankce případně uložené z tohoto důvodu Objednateli ze strany Úřadu pro ochranu osobních údajů či jiným správním orgánem, který bude v budoucnu vykonávat působnost Úřadu pro ochranu osobních údajů. Objednatel je však za předpokladu, že mu k tomu Dodavatel poskytne nezbytnou součinnost, povinen uplatnit v příslušných řízeních veškeré přiměřené námitky, které mohl uplatnit ve svém zájmu, a v rámci řízení je povinen řádně hájit svá práva.

22. OCHRANA DŮVĚRNÝCH INFORMACÍ

- 22.1. Dodavatel se zavazuje zachovávat mlčenlivost o všech Důvěrných informacích, které získal nebo mu byly poskytnuty či zpřístupněny v souvislosti s plněním povinností dle Smlouvy, a uchovávat je v tajnosti.
- 22.2. Dodavatel se zavazuje použít Důvěrné informace pouze k plnění svých povinností vyplývajících ze Smlouvy. Dodavatel nesmí použít Důvěrné informace k jinému účelu.
- 22.3. Dodavatel nesmí bez předchozího písemného souhlasu Objednatele zpřístupnit Důvěrné informace žádné třetí osobě, a to v jakékoli formě. To neplatí u Důvěrných informací, ohledně kterých byla Dodavateli pravomocným rozhodnutím soudu, správního orgánu, či jiného příslušného státního orgánu v konkrétním případě uložena povinnost Důvěrnou informaci poskytnout nebo plyne-li taková povinnost Dodavateli z právního předpisu.
- 22.4. Dodavatel nesmí Důvěrné informace bez předchozího písemného souhlasu Objednatele rozmnožovat, kopírovat či jakýmkoliv jiným způsobem reprodukovat. Dodavatel dále nesmí Důvěrné informace bez předchozího písemného souhlasu Objednatele uchovávat v jakékoliv databázi, počítačovém programu, úložišti či na datovém nosiči, vyjma případů, kdy je takové uchování Důvěrných informací nezbytné pro účel vyplývající ze Smlouvy.
- 22.5. Dodavatel se zavazuje provést technická, organizační, právní a personální opatření, kterými zajistí dodržování povinnosti zachovat mlčenlivost o Důvěrných informacích a uchovat Důvěrné informace v tajnosti v rozsahu podle tohoto článku i ze strany svých zaměstnanců, Poddodavatelů, jakož i dalších osob, kterým budou Důvěrné informace poskytnuty či zpřístupněny.
- 22.6. Objednatel je oprávněn kdykoliv kontrolovat řádné plnění povinností Dodavatele uvedených v tomto článku, k čemuž se Dodavatel zavazuje bez zbytečného odkladu poskytnout Objednateli veškerou součinnost, zejména je Objednatel oprávněn kontrolovat řízení bezpečnosti Důvěrných informací Dodavatelem. V případě, že Objednatel vyzve Dodavatele na základě kontroly k nápravě, je Dodavatel povinen takové výzvě vyhovět v Objednatelem stanovené přiměřené lhůtě.
- 22.7. Objednatel je oprávněn požadovat na Dodavateli zaplacení smluvní pokuty:
(a) ve výši 500 000 Kč za každé jednotlivé jednání, které představuje porušení jakékoli z povinností Dodavatele dle tohoto článku, vyjma povinností stanovených v článku 22.6. ZOP
(a) ve výši 100 000 Kč za každé jednotlivé jednání, které představuje porušení jakékoli z povinností stanovených v článku 22.6. ZOP.

Obchodní podmínky ke Smlouvě o dílo

OBSAH OBCHODNÍCH PODMÍNEK

ČÁST 1 - ÚVODNÍ USTANOVENÍ.....	2
ČÁST 2 - NÁVRH NA UZAVŘENÍ SMLOUVY O DÍLO	3
ČÁST 3 - DÍLO	3
ČÁST 4 - CENA DÍLA	4
ČÁST 5 - ZMĚNA CENY DÍLA.....	4
ČÁST 6 - PLATEBNÍ PODMÍNKY	5
ČÁST 7 - MÍSTO PLNĚNÍ.....	5
ČÁST 8 - DOBA PLNĚNÍ	5
ČÁST 9 - PROVÁDĚNÍ DÍLA.....	6
ČÁST 10 - ZKUŠEBNÍ PROVOZ	8
ČÁST 11 - PŘEPRAVA DÍLA	8
ČÁST 12 - PODDODAVATELÉ	9
ČÁST 13 - PŘEDÁNÍ A PŘEVZETÍ DÍLA	9
ČÁST 14 - VLASTNICKÉ PRÁVO A NEBEZPEČÍ ŠKODY	11
ČÁST 15 - VADY PLNĚNÍ A ZÁRUKA	11
ČÁST 16 - UPLATNĚNÍ PRÁV Z VADNÉHO PLNĚNÍ	12
ČÁST 17 - PODMÍNKY ODSTRANĚNÍ VAD	12
ČÁST 18 - POJIŠTĚNÍ	13
ČÁST 19 - DUŠEVNÍ VLASTNICTVÍ	13
ČÁST 20 - SANKCE.....	14
ČÁST 21 - OBECNÁ ODPOVĚDNOST ZHOTOVITELE	15
ČÁST 22 - Odstoupení od smlouvy o dílo.....	15
ČÁST 23 - OSTATNÍ UJEDNÁNÍ.....	16

ČÁST 1 - ÚVODNÍ USTANOVENÍ

1. Pro účely těchto Obchodních podmínek mají následující slova význam u nich uvedený:
 - 1.1. **Občanský zákoník** – zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
 - 1.2. **ZoDPH** – zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
 - 1.3. **ZoÚ** – zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
 - 1.4. **SZ** – zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon), ve znění pozdějších předpisů.
 - 1.5. **ZZVZ** – zákon č. 134/2016 Sb., o zadávání veřejných zakázkách, ve znění pozdějších předpisů.
 - 1.6. **Objednatel** – Správa železnic, státní organizace, IČO 70994234, se sídlem Praha 1 – Nové Město, Dlážděná 1003/7, PSČ 110 00, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 48384.
 - 1.7. **Zhotovitel** – osoba uvedená ve Smlouvě o dílo jako Zhotovitel; též všechny osoby, které jsou ve Smlouvě o dílo uvedené na straně Zhotovitele, je-li na straně Zhotovitele více než jedna osoba.
 - 1.8. **Smluvní strany** – Objednatel a Zhotovitel.
 - 1.9. **Smluvní strana** – Objednatel nebo Zhotovitel dle smyslu ujednání.
 - 1.10. **Nabídka** – souhrn dokumentů, které Zhotovitel podal jako návrh do zadávacího řízení, na jehož základě byla uzavřena Smlouva o dílo.
 - 1.11. **Smlouva o dílo** – smlouva uzavřená mezi Smluvními stranami, která odkazuje na Obchodní podmínky.
 - 1.12. **Obchodní podmínky** – tento text obchodních podmínek.
 - 1.13. **Předmět díla** – věc, která má být zhotovena, nebo činnost s jiným výsledkem, specifikovaná ve Smlouvě o dílo.
 - 1.14. **Související plnění** – další plnění (práce, dodávky, služby, činnosti a výkony), která je Zhotovitel povinen dle Smlouvy o dílo poskytnout vedle samotného provedení Předmětu díla.
 - 1.15. **Rozhodnutí Objednatele** – veškerá rozhodnutí, sdělení, souhlasy, povolení či jiné výsledky úkonů orgánů státní správy, samosprávy či jiných subjektů, které pro účely Díla nebo v souvislosti s ním získal nebo do doby dokončení Díla získá Objednatel a jež Objednatel Zhotoviteli předal nebo s nimiž se Zhotovitel jinak seznámil.
 - 1.16. **Rozhodnutí Zhotovitele** – veškerá rozhodnutí, sdělení, souhlasy, povolení či jiné výsledky úkonů orgánů státní správy, samosprávy či jiných subjektů, které je Zhotovitel povinen dle Smlouvy o dílo získat. Jakékoliv Rozhodnutí Zhotovitele, které není v českém jazyku, musí být do českého jazyka přeloženo a překlad musí být úředně ověřen.
 - 1.17. **Veřejnoprávní podklady** – souhrn Rozhodnutí Objednatele a Rozhodnutí Zhotovitele.
 - 1.18. **Doklady** – veškeré listiny, které se vztahují k Předmětu díla nebo Souvisejícímu plnění a které jsou třeba k jejich převzetí a užívání; veškerá Rozhodnutí Zhotovitele; veškeré další listiny, vyjma Výzvy k úhradě, které je Zhotovitel dle Smlouvy o dílo povinen předat Objednateli. Všechny Doklady musejí být v českém jazyku, nebo v původním jazyku s překladem do českého jazyka, není-li uvedeno jinak.
 - 1.19. **Dílo** – souhrn veškerých plnění, která je Zhotovitel povinen provést za účelem splnění Smlouvy o dílo; zahrnuje zejm. provedení Předmětu díla, poskytnutí či provedení Souvisejícího plnění a dodání Dokladů.
 - 1.20. **Cena díla** – cena za Dílo sjednaná ve Smlouvě o dílo (částka bez DPH).
 - 1.21. **Výzva k úhradě** – daňový doklad, je-li Zhotovitel povinen dle ZoDHP uhradit v souvislosti s provedením Díla nebo jeho části DPH, nebo faktura, pokud

Zhotovitel v souvislosti s provedením Díla nebo jeho části není dle ZoDPH povinen uhradit DPH.

- 1.22. **Vícepráce** – práce, dodávky nebo služby nad rámec Smlouvy o dílo, na jejichž provedení se Smluvní strany dohodnou po uzavření Smlouvy o dílo.
- 1.23. **Méněpráce** – práce, dodávky nebo služby v rámci Smlouvy o dílo, na jejichž vypuštění se Smluvní strany dohodnou po uzavření Smlouvy o dílo.
- 1.24. **Obalový materiál** – palety, dřevěné desky či jiné věci, které slouží pro potřeby přepravy nebo ochrany Předmětu díla. Dle kontextu Smlouvy o dílo se rozumí Obalovým materiálem též jednotlivý kus palety, dřevěné desky nebo jiné věci.
- 1.25. **Přejímací řízení** – proces, při kterém Zhotovitel předává a Objednatel kontroluje a přebírá Dílo, nebo je odmítá.
- 1.26. **Předávací protokol** – listina osvědčující předání a převzetí Díla nebo jeho části, jejíž minimální náležitosti jsou uvedeny v části Předání a převzetí Díla.
- 1.27. **Záruční doba** – doba, do jejíhož uplynutí je Objednatel oprávněn uplatňovat práva z vad plnění poskytnutého Zhotovitelem na základě Smlouvy o dílo; Záruční doba činí 24 měsíců.
- 1.28. **CTD** – Centrum telematiky a diagnostiky, organizační jednotka Objednatele.

ČÁST 2 - NÁVRH NA UZAVŘENÍ SMLOUVY O DÍLO

- 2. Odpověď Smluvní strany na návrh na uzavření Smlouvy o dílo učiněný druhou Smluvní stranou, která vymezuje obsah návrhu jinými slovy nebo která obsahuje jakékoliv, byť nepodstatné, dodatky, odchylky, výhrady nebo omezení není přijetím návrhu.
- 3. I pozdní přijetí návrhu na uzavření Smlouvy o dílo má účinky včasného přijetí, pokud navrhuje Smluvní strana bez zbytečného odkladu alespoň ústně vyrozumí druhou Smluvní stranu, že přijetí považuje za včasné, nebo pokud se začne chovat ve shodě s návrhem.
- 4. Plyne-li z písemnosti, která vyjadřuje přijetí návrhu na uzavření Smlouvy o dílo, že byla odeslána za takových okolností, že by došla navrhuje Smluvní straně včas, kdyby její přeprava probíhala obvyklým způsobem, má pozdní přijetí účinky včasného přijetí, ledaže navrhuje Smluvní strana bez odkladu vyrozumí alespoň ústně druhou Smluvní stranu, že považuje návrh za zaniklý.
- 5. Bez ohledu na jakékoliv okolnosti nelze přijmout návrh na uzavření Smlouvy o dílo tak, že se Smluvní strana, již je návrh určen, podle návrhu zachová.
- 6. **Odkáží-li Smluvní strany v návrhu na uzavření Smlouvy o dílo i v přijetí návrhu na obchodní podmínky, které si odporují, je Smlouva o dílo přesto uzavřena s obsahem určeným v tom rozsahu, v jakém obchodní podmínky nejsou v rozporu; to platí i v případě, že to obchodní podmínky vylučují. Vyloučí-li to některá ze Smluvních stran nejpozději bez zbytečného odkladu po výměně projevů vůle, Smlouva o dílo uzavřena není.**
- 7. Smlouva o dílo může být uzavřena pouze v písemné podobě.

ČÁST 3 - DÍLO

- 8. Zhotovitel se zavazuje provést na svůj náklad a nebezpečí pro Objednatele Dílo a Objednatel se zavazuje Dílo převzít a zaplatit Zhotoviteli Cenu díla a příslušnou DPH, bude-li Zhotovitel povinen dle ZoDHP uhradit v souvislosti s provedením Díla nebo jeho části DPH.
- 9. Zhotovitel je povinen provést Dílo v jakosti, provedení a způsobem uvedeným ve Smlouvě o dílo a zároveň
 - 9.1. v jakosti, provedení a způsobem, jenž odpovídá vlastnostem a způsobu, které Zhotovitel popsal nebo které Objednatel očekával s ohledem na povahu Díla, a to v rozsahu, ve kterém není v rozporu s jakostí, provedením a způsobem sjednaným ve Smlouvě o dílo,
 - 9.2. v jakosti, provedení a způsobem, jenž se hodí k účelu vyplývajícimu ze Smlouvy o dílo a není-li v ní vyjádřen pak k účelu, ke kterému se Dílo obvykle používá, a

- to v rozsahu, ve kterém není v rozporu s jakostí, provedením a způsobem sjednaným ve Smlouvě o dílo,
- 9.3. v souladu s Veřejnoprávními podklady,
 - 9.4. v souladu s požadavky právních předpisů a příslušných ČSN.
- 10. Je-li jakost či provedení Předmětu díla zároveň určeno vzorkem nebo předlohou, musí Předmět díla odpovídat jakostí nebo provedením vzorku nebo předloze. Liší-li se jakost nebo provedení určené ve Smlouvě o dílo a vzorek nebo předloha, rozhoduje Smlouva o dílo. Určuje-li Smlouva o dílo a vzorek nebo předloha jakost nebo provedení rozdílně, nikoliv však rozporně, musí Předmět díla odpovídat Smlouvě o dílo i vzorku nebo předloze.
 - 11. Opatruje-li Zhotovitel věc za účelem jejího zpracování při provádění Díla, je povinen opatřit věc novou, nepoužitou a neopotřebovanou.
 - 12. Je-li součástí Díla povinnost Zhotovitele zajistit jakékoliv Rozhodnutí Zhotovitele, je Zhotovitel povinen provést veškeré činnosti, kterých je k získání příslušného Rozhodnutí Zhotovitele třeba.

ČÁST 4 - CENA DÍLA

- 13. Cena díla zahrnuje veškeré náklady Zhotovitele spojené se splněním jeho povinností vyplývajících ze Smlouvy o dílo a Obchodních podmínek a zisk Zhotovitele.
- 14. Objednatel není povinen hradit v souvislosti se Smlouvou o dílo žádné jiné finanční částky, než Cenu díla a případně příslušnou DPH, není-li uvedeno jinak (tím není dotčeno právo Zhotovitele na případnou úhradu smluvní pokuty, úroků z prodlení, či jiných sankcí, a právo na náhradu škody způsobené Objednatelem).
- 15. Cena díla obsahuje předpokládaný vývoj cen vstupních nákladů a předpokládané zvýšení ceny v závislosti na čase plnění, a to až do dokončení Díla.
- 16. Je-li Zhotovitel povinen dle ZoDHP uhradit v souvislosti s provedením Díla nebo jeho části DPH, je Objednatel povinen Zhotoviteli takovou DPH uhradit vedle Ceny díla.
- 17. Cenu díla lze měnit pouze za podmínek uvedených v části Změna ceny Díla (viz ČÁST 5 - Obchodních podmínek).
- 18. Konečné finanční částky na fakturách/daňových dokladech nesmí být zaokrouhlovány na celé Kč. Objednatel nebude akceptovat zaokrouhlení a haléřové vyrovnání v případě uvedení na faktuře/daňovém dokladu nebude hradit.

ČÁST 5 - ZMĚNA CENY DÍLA

- 19. Změna ceny díla je možná pouze v případě
 - 19.1. víceprací nebo méněprací,
 - 19.2. zjistí-li Zhotovitel při kontrole projektové dokumentace předané mu Objednatelem vady nebo její nevhodnost či neúplnost, které mají vliv na náklady Zhotovitele,
 - 19.3. v jiných případech jen pokud se na tom Smluvní strany dohodnou.
- 20. V případě víceprací i méněprací Zhotovitel provede ocenění jejich soupisu jednotkovými cenami položkového rozpočtu, je-li ve Smlouvě o dílo zahrnut.
- 21. Pokud práce, dodávky nebo služby nebudou v položkovém rozpočtu obsaženy nebo položkový rozpočet není ve Smlouvě o dílo zahrnut, užije se pro jejich ocenění cena obvyklá.
- 22. V případě vad, nevhodnosti nebo neúplnosti projektové dokumentace, kterou předal Objednatel Zhotoviteli, je-li taková projektová dokumentace součástí Smlouvy o dílo, mají-li takové vady, nevhodnosti nebo neúplnosti vliv na náklady Zhotovitele, postupují smluvní strany obdobně jako při oceňování víceprací nebo méněprací.
- 23. Změnu Ceny díla lze provést jen uzavřením dodatku ke Smlouvě o dílo.

ČÁST 6 - PLATEBNÍ PODMÍNKY

24. Objednatel neposkytuje zálohy.
25. Zhotovitel vyúčtuje Objednateli Cenu díla a případnou DPH Výzvou k úhradě.
26. Cenu díla a případnou DPH je Objednatel povinen uhradit Zhotoviteli do 30 dnů ode dne převzetí Díla; má-li být dle Smlouvy o dílo proveden též zkušební provoz, pak do 30 dnů ode dne úspěšného ukončení zkušebního provozu, nastane-li den skončení zkušebního provozu později než převzetí Díla Objednatel.
27. Cena díla a případná DPH je uhrazena dnem jejich odepsání z bankovního účtu Objednatele.
28. Je-li Výzva k úhradě fakturou, musí obsahovat náležitosti účetního dokladu dle §11 ZoÚ a náležitosti stanovené v §435 Občanského zákoníku.
29. Je-li Výzva k úhradě daňovým dokladem, musí obsahovat náležitosti daňového dokladu dle §28 ZoDPH a náležitosti stanovené v §435 Občanského zákoníku.
30. Výzva k úhradě musí vždy obsahovat číslo Smlouvy o dílo, včetně uvedení uzavřených dodatků, její přílohou musí být vždy jedno vyhotovení Protokolu o převzetí potvrzeného Objednatel. Ve výzvě k úhradě musí být vždy uvedeny jako identifikace Objednatele nejméně následující údaje:
Správa železnic, státní organizace
Dlážděná 1003/7, 110 00 Praha 1 – Nové Město
IČO: 709 94 234
Obchodní rejstřík u Městského soudu v Praze, sp. zn. A 48384
31. Výzvu k úhradě je Zhotovitel povinen doručit Objednateli **ve dvou vyhotoveních** nejpozději 15 dnů před uplynutím doby uvedené v odstavci 25 Obchodních podmínek.
32. Splatnost Výzvy k úhradě musí být stanovena tak, aby nastala dříve, než uplyne doba stanovená v odstavci 25 Obchodních podmínek.
33. Stanoví-li Výzva k úhradě splatnost delší, než je jako minimální stanovena v předchozím odstavci, je Objednatel oprávněn uhradit Cenu díla a případnou DPH ve lhůtě splatnosti určené ve Výzvě k úhradě.
34. Stane-li se zhotovitel nespolehlivým plátcem nebo daňový doklad zhotovitele bude obsahovat číslo bankovního účtu, na který má být plněno, aniž by bylo uvedeno ve veřejném registru spolehlivých účtů, je objednatel oprávněn z finančního plnění uhradit daň z přidané hodnoty přímo místně a věcně příslušnému správci daně zhotovitele.
35. Je-li ve Smlouvě o dílo výslovně stanoveno, že Zhotovitel bude předávat Objednateli Dílo po částech, je Zhotovitel oprávněn vystavit Výzvu k úhradě předávané části Díla poté, co Objednatel převezme příslušnou část Díla. Ustanovení odstavců 26 - 33 Obchodních podmínek se užijí obdobně.
36. Ustanovení §2611, §2620–2622 a §2624 Občanského zákoníku se neužijí.

ČÁST 7 - MÍSTO PLNĚNÍ

37. Zhotovitel je povinen předat Objednateli Dílo v místě, jež vyplývá ze Smlouvy o dílo. Nelze-li takto místo předání Díla zjistit, vyzve Zhotovitel Objednatele, aby sdělil, ve kterém místě má Zhotovitel Objednateli Dílo předat. Nesdělí-li Objednatel místo plnění do 5 pracovních dnů ode dne doručení výzvy Zhotovitele, je Zhotovitel povinen Dílo předat Objednateli v sídle Objednatele.

ČÁST 8 - DOBA PLNĚNÍ

38. Zhotovitel je povinen zahájit provádění Díla bez zbytečného odkladu po uzavření Smlouvy o dílo.
39. Je-li součástí povinností Zhotovitele doprava Díla po jeho zhotovení do místa plnění dle Smlouvy o dílo, je Zhotovitel povinen dopravit Dílo do místa plnění v pracovní den v době od 8 do 15 hodin. Dodá-li Zhotovitel Dílo Objednateli v jiné než uvedené době, je Objednatel oprávněn odmítnout Dílo převzít a není zároveň v prodlení s převzetím Díla. Případně-li konec sjednané doby plnění na sobotu, neděli nebo svátek, není Zhotovitel

v prodlení, dodá-li Dílo nejbližší následující pracovní den v časovém rozmezí dle tohoto odstavce.

- 40. Není-li stanoveno jinak, je Zhotovitel povinen začít s plněním svých povinností vždy bez zbytečného odkladu.
- 41. Zjistí-li Zhotovitel jakékoliv skutečnosti, které by mohly mít vliv na dobu plnění, je Zhotovitel povinen bez zbytečného odkladu Objednatele o takových skutečnostech informovat.

ČÁST 9 - PROVÁDĚNÍ DÍLA

- 42. Zhotovitel provede Dílo s potřebnou péčí v ujednaném čase a obstará vše, co je k provedení Díla potřeba.
- 43. Při provádění Díla postupuje Zhotovitel samostatně, je však vázán příkazy Objednatele ohledně způsobu provádění Díla.
- 44. Zhotovitel se zavazuje brát v úvahu veškeré upozornění Objednatele, týkající se realizace Díla a upozorňující na možné porušování smluvních i právními předpisy stanovených povinností Zhotovitele.
- 45. Zhotovitel je povinen upozornit Objednatele bez zbytečného odkladu na nevhodnou povahu věcí převzatých od Objednatele nebo příkazů daných mu Objednatelem k provedení Díla, jestliže Zhotovitel mohl tuto nevhodnost zjistit při vynaložení odborné péče.
- 46. Překáží-li nevhodná věc nebo příkaz v řádném provádění Díla, Zhotovitel je v nezbytném rozsahu přeruší až do výměny věci nebo změny příkazu; trvá-li Objednatel na provádění Díla s použitím předané věci nebo podle daného příkazu, má Zhotovitel právo požadovat, aby tak Objednatel učinil v písemné formě.
- 47. Doba stanovená pro dokončení Díla se prodlužuje o dobu vyvolanou přerušením dle předchozího odstavce.
- 48. Trvá-li Objednatel na provádění Díla s použitím předané věci nebo podle daného příkazu a zachová-li se Zhotovitel podle toho, nemá Objednatel práva z vady Díla vzniklé pro nevhodnost věci nebo příkazu.

Harmonogram

- 49. Je-li dle Smlouvy o dílo vyžadován Harmonogram provádění Díla, je Zhotovitel povinen jej předložit Objednateli bez zbytečného odkladu po uzavření Smlouvy o dílo, nejpozději však do 10 dnů ode dne uzavření Smlouvy o dílo.
- 50. Zhotovitel je povinen udržovat harmonogram v aktuálním stavu a v případě změny vždy předat Objednateli bezodkladně aktualizovaný harmonogram.

Kontrola provádění prací

- 51. Objednatel je oprávněn kontrolovat provádění Díla. Zjistí-li objednatel, že Zhotovitel provádí Dílo v rozporu s povinnostmi vyplývajícími ze Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů nebo příslušných ČSN, je Objednatel oprávněn dožadovat se toho, aby Zhotovitel odstranil vady vzniklé vadným prováděním a Dílo prováděl řádným způsobem. Jestliže tak Zhotovitel neučiní v přiměřené lhůtě, jedná se o podstatné porušení Smlouvy o dílo.
- 52. Zhotovitel je povinen písemně vyzvat Objednatele ke kontrole a prověření prací, které v dalším postupu budou zakryty nebo se stanou nepřístupnými. Zhotovitel je povinen vyzvat Objednatele nejméně 3 pracovní dny před termínem, v němž budou předmětné práce zakryty nebo zneprístupněny.
- 53. Před zakrytím nebo zneprístupněním prací je Zhotovitel povinen pořídit podrobnou fotodokumentaci prací a předat ji Objednateli v digitální podobě na CD nebo DVD nosiči bez zbytečného odkladu po pořízení fotodokumentace.
- 54. Pokud se Objednatel ke kontrole přes včasné písemné vyzvání nedostaví, je Zhotovitel oprávněn předmětné práce zakrýt. Bude-li se v tomto případě Objednatel dodatečně požadovat jejich odkrytí, je Zhotovitel povinen toto odkrytí provést na náklady Objednatele. Pokud se však zjistí, že práce nebyly řádně provedeny, nese veškeré náklady spojené s odkrytím prací, opravou chybného stavu a následným zakrytím Zhotovitel.

55. Obdobně bude-li Objednatel požadovat vykonání zvláštních zkoušek nebo ověření jakékoliv části Díla z důvodu podezření, že tato část Díla neodpovídá Smlouvě o dílo, Obchodním podmínkám, Veřejnoprávním podkladům, právním předpisům nebo příslušným ČSN, a bude-li zjištěno, že podezření bylo správné, nese náklady spojené s vykonáním zkoušek nebo ověřením Zhotovitel.

56. Zhotovitel je povinen umožnit výkon technického a autorského dozoru.

Kontrolní dny

57. Pro účely kontroly průběhu provádění Díla může Objednatel nebo jím pověřená osoba provést kontrolní dny v termínech nezbytných pro řádné provádění kontroly.
58. Kontrolních dnů se zúčastní zástupci Objednatele případně osob vykonávajících funkci technického dozoru a autorského dozoru.
59. Zástupci Zhotovitele jsou povinni se kontrolních dnů zúčastňovat. Zhotovitel má právo přizvat na kontrolní den své poddodavatele podílející se v souladu se Smlouvou o dílo a Obchodními podmínkami na provádění Díla.
60. Kontrolní dny vede Objednatel nebo jím pověřená osoba.
61. Obsahem kontrolního dne je zejména zpráva Zhotovitele o postupu prací, kontrola postupu prací, připomínky a podněty osob vykonávajících funkci technického a autorského dozoru a stanovení případných nápravných opatření a úkolů.
62. Objednatel nebo jím pověřená osoba pořizuje z kontrolního dne zápis, který předá všem zúčastněným.

Dodržování zákazu požívání alkoholických nápojů a užívání jiných návykových látek

63. Objednatel je oprávněn provádět u všech osob, které Zhotovitel používá při provádění díla, kontrolu, zda tyto osoby nejsou pod vlivem alkoholu nebo návykové látky.
64. Kontrola bude prováděna dle Směrnice SŽDC č. 120 Dodržování zákazu kouření, požívání alkoholických nápojů a užívání jiných návykových látek, č.j. 36503/2017-SŽDC-GR-O10 ze dne 3.11.2017, účinné od 7.11.2017 nebo dle jiného předpisu, který uvedenou směrnici případně nahradí.
65. Výše uvedená Směrnice je pro Zhotovitele a všechny osoby, které Zhotovitel používá při provádění Předmětu Díla závazná okamžikem platnosti a účinnosti Smlouvy o dílo. Zhotovitel a tím i všechny osoby, které Zhotovitel používá při provádění Předmětu Díla, se zavazují poskytnout Objednateli veškerou součinnost v souladu s výše uvedenou směrnicí.

Dodržování podmínek stanovisek příslušných orgánů a organizací

66. Zhotovitel se zavazuje dodržet při provádění Díla veškeré podmínky vyplývající z Veřejnoprávních podkladů.
67. Pokud nesplněním těchto podmínek vznikne Objednateli škoda, je Zhotovitel povinen nahradit škodu v plném rozsahu, ledaže prokáže, že škodě nemohl zabránit ani v případě vynaložení veškeré možné péče, kterou na něm lze spravedlivě požadovat.

Použité materiály a výrobky

68. Zhotovitel se zavazuje a odpovídá za to, že při realizaci Díla nepoužije žádný materiál, o kterém je v době jeho užití známo, že je škodlivý. Pokud tak Zhotovitel učiní, je povinen na vyzvání Objednatele provést nápravu, přičemž veškeré náklady s tím spojené nese Zhotovitel.
69. Zhotovitel se zavazuje, že k realizaci Díla nepoužije materiály, které nemají požadovanou certifikaci či předepsaný průvodní doklad, je-li to pro jejich použití nezbytné podle Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů nebo příslušných ČSN. Certifikace a průvodní doklady Zhotovitele použitých materiálů jsou součástí Dokladů.

Částečné plnění

70. Nabízí-li Zhotovitel Objednateli částečné plnění Předmětu díla, aniž by částečné plnění bylo výslovně sjednáno ve Smlouvě o dílo, není Objednatel povinen částečné plnění přijmout. Přijme-li Objednatel částečné plnění, je Zhotovitel povinen nahradit Objednateli zvýšené náklady způsobené mu částečným plněním.

Ostatní ujednání

71. Vícepráce lze provést a méněpráce neprovést až poté, co budou vícepráce nebo méněpráce dohodnuty včetně změn Ceny díla dodatkem ke Smlouvě o dílo. Provede-li Zhotovitel vícepráce v rozporu s tímto odstavcem, ponese náklady na ně ze svého.
72. Dojde-li k jakémukoliv úrazu při provádění Díla nebo při činnostech souvisejících s prováděním Díla je Zhotovitel povinen zabezpečit vyšetření úrazu a sepsání příslušného záznamu. Objednatel je povinen poskytnout Zhotoviteli nezbytnou součinnost.
73. Žádný z podkladů, které Zhotovitel převzal od Objednatele v souvislosti s Dílem ani žádný Doklad není Zhotovitel oprávněn bez předchozího písemného svolení Objednatele užít k jiným účelům, než je provedení Díla, zejména je nesmí poskytnout třetím osobám.
74. Zhotovitel je povinen při provádění Díla postupovat v součinnosti s případnými jinými dodavateli Objednatele, a to dle pokynů udělených Objednatelem a nebudou-li pokyny uděleny, postupovat tak, aby umožnil ostatním dodavatelům v co největší míře plnit jejich závazky.
75. Objednatel se zavazuje poskytovat Zhotoviteli součinnost při provádění Díla v rozsahu a způsobem, ve kterém lze tuto součinnost po Objednateli spravedlivě požadovat. Bude-li Zhotovitelem požadována po Objednateli jakákoliv součinnost dle předchozí věty, je Zhotovitel povinen Objednatele k jejímu poskytnutí s dostatečným předstihem vyzvat a ve výzvě ji dostatečně specifikovat.
76. Zhotovitel na sebe přebírá nebezpečí změny okolností ve smyslu §1765 Občanského zákoníku.
77. Ustanovení §1912, §2595 Občanského zákoníku se neužijí.

ČÁST 10 - ZKUŠEBNÍ PROVOZ

78. Ustavení této části se užijí v případě, že ze Smlouvy o dílo nebo z povahy Předmětu díla vyplývá, že má být proveden zkušební provoz.
79. Zkušebním provozem se prověřuje, zda Předmět díla je za předpokládaných provozních a výrobních podmínek schopen dosahovat výkonů (parametrů) v kvalitě a množství stanovených Smlouvou o dílo, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN.
80. Zkušební provoz je Zhotovitel povinen provést před předáním Díla Objednateli, do doby úspěšného provedení zkušebního provozu není Dílo dokončeno.
81. Zkušební provoz musí trvat minimálně 48 hodin, nestanoví-li Veřejnoprávní podklady, právní předpisy nebo příslušné ČSN jinak.
82. Zhotovitel se zavazuje v průběhu zkušebního provozu neprodleně odstraňovat veškeré vady, které bude Předmět díla vykazovat.
83. Zkušební provoz bude úspěšně proveden, nebude-li Předmět díla k poslednímu dni doby stanovené pro zkušební provoz vykazovat vady bránící jeho užívání.
84. Bude-li k poslednímu dni doby zkušebního provozu Předmět díla vykazovat vady bránící užívání, prodlužuje se délka trvání zkušebního provozu o dobu dle dohody Smluvních stran, jinak o 24 hodin.
85. Úspěšné provedení zkušebního provozu je podmínkou převzetí díla Objednatelem.

ČÁST 11 - PŘEPRAVA DÍLA

86. Ustavení této části se užijí v případě, je-li Dílo po svém zhotovení za účelem předání Objednateli přepravováno.
87. Je-li dle Smlouvy o dílo nebo zvyklostí třeba Předmět díla zabalit, Zhotovitel Předmět díla zabalí dle Smlouvy o dílo; není-li ujednání o balení Předmětu díla ve Smlouvě o dílo, pak dle zvyklostí, a není-li jich, pak způsobem potřebným pro uchování Předmětu díla a jeho ochranu.
88. Jestliže Zhotovitel označí Obalový materiál nejpozději do doby převzetí Předmětu díla Objednatelem jako vratný, a to přímo na Obalovém materiálu, v Dokladech nebo jiným zřejmým způsobem, ze kterého bude zřejmé, který Obalový materiál je vratný, je Objednatel oprávněn předat Zhotoviteli při předávacím řízení (viz ČÁST 13 - Obchodních podmínek) stejné množství Obalového materiálu téhož druhu a srovnatelného nebo

- nižšího stupně opotřebení. V rozsahu předání Obalového materiálu Objednatel Zhotoviteli dle předchozí věty zaniká právo Zhotovitele na vrácení Obalového materiálu.
89. V rozsahu, v němž Objednatel nevrátí vratný Obalový materiál Zhotoviteli dle předchozího odstavce, je Zhotovitel oprávněn Objednateli vyúčtovat zálohu na vratný Obalový materiál. Výše zálohy nesmí přesáhnout dvojnásobek pořizovací ceny Obalového materiálu.
90. Doposud nevrácený vratný Obalový materiál je Objednatel povinen na vlastní náklady dopravit do sídla Zhotovitele, a to nejpozději do jednoho roku od převzetí Předmětu díla Objednatel. Objednatel je oprávněn nahradit nevrácený vratný Obalový materiál Obalovým materiálem stejného druhu a srovnatelného nebo nižšího stupně opotřebení. Bez zbytečného odkladu po převzetí vráceného Obalového materiálu nebo jeho náhrady Zhotovitelem, je Zhotovitel povinen vrátit Objednateli zaplacenou zálohu na vratný Obalový materiál. Nevratí-li Objednatel dosud nevrácený vratný Obalový materiál nebo Obalový materiál stejného druhu a srovnatelného nebo nižšího stupně opotřebení ani do dvou let od převzetí Předmětu díla Objednatel, stává se nevrácený vratný Obalový materiál vlastnictvím Objednatele a složená záloha se stává vlastnictvím Zhotovitele.
91. Pokud Zhotovitel Předmět díla Objednateli odesílá prostřednictvím dopravce, umožní Zhotovitel Objednateli uplatnit práva z přepravní smlouvy vůči dopravci, pokud o to Objednatel Zhotovitele požádá.
92. Pokud Zhotovitel Předmět díla Objednateli odesílá prostřednictvím dopravce, je Zhotovitel povinen zajistit dopravu u dopravce tak, aby Předmět díla byl dodán Objednateli v době uvedená v odstavci 39 Obchodních podmínek.
93. Je-li třeba provést vyložení Předmětu díla z dopravního prostředku, je vyložení povinen provést Zhotovitel na své náklady.
94. Je-li Objednatel v prodlení s převzetím Předmětu díla, uchová jej Zhotovitel, může-li s ním nakládat, pro Objednatele způsobem přiměřeným okolnostem. Převzal-li Objednatel Předmět díla, který zamýšlí odmítnout, uchová jej způsobem přiměřeným okolnostem. Smluvní strana, která uchovává Předmět díla pro druhou Smluvní stranu, má právo na náhradu účelně vynaložených nákladů spojených s uchováním Předmětu díla, nemůže jej však za účelem zajištění svého práva na úhradu nákladů zadržet.

ČÁST 12 - PODDODAVATELÉ

95. Zhotovitel je oprávněn pověřit provedením části Díla třetí osobu – poddodavatele. Zhotovitel odpovídá za činnost poddodavatele tak, jako by činnost prováděl sám.
96. Zhotovitel je oprávněn pověřit provedením části Díla poddodavatele pouze, pokud je poddodavatel uveden v příloze Smlouvy o dílo.
97. Zhotovitel se zavazuje, že poddodavatelé splní všechny povinnosti vyplývající Zhotoviteli ze Smlouvy o dílo, a to přiměřeně k povaze a rozsahu poddodávky.
98. Zhotovitel se zavazuje, že poddodavatelé, kterými prokazoval splnění kvalifikace v zadávacím řízení, se budou podílet na provedení příslušné věcně vymezené části Díla v rozsahu dle Nabídky Zhotovitele.
99. Zhotovitel je oprávněn změnit poddodavatele pouze s předchozím písemným souhlasem Objednatele. Objednatel vydá písemný souhlas se změnou do 10 dnů od doručení žádosti Zhotovitele. Objednatel souhlas se změnou nevydává, pokud
- 99.1. prostřednictvím původního poddodavatele Zhotovitel v zadávacím řízení prokazoval kvalifikaci a nový poddodavatel nebude mít stejnou či vyšší kvalifikaci jako původní nahrazovaný poddodavatel nebo
- 99.2. po Objednateli nelze spravedlivě požadovat, aby s takovou změnou souhlasil.

ČÁST 13 - PŘEDÁNÍ A PŘEVZETÍ DÍLA

100. Závazek Zhotovitele provést Dílo je splněn jeho dokončením a převzetím Díla Objednatel, včetně převzetí veškerých Dokladů.
101. Součástí Dokladů je dle povahy a charakteru Díla též
- 101.1. dodavatelská výrobní a dílenská dokumentace,

- 101.2. atesty, záruční listy, prohlášení o shodě všech věcí, jež byly použity při provádění Díla,
 - 101.3. zápisy a osvědčení o všech předepsaných zkouškách, měřeních,
 - 101.4. dokumenty osvědčující průběh zkušebního provozu,
 - 101.5. servisní plán, návod k obsluze a návod k použití částí Díla,
 - 101.6. doklady o zabezpečení likvidace odpadů v souladu s právními předpisy,
 - 101.7. fotodokumentace z průběhu provádění Díla, zejména fotodokumentace prací a konstrukcí, které byly dalším postupem prací zakryté nebo jinak zneprístupněné,
102. V případě, že Smlouva o dílo, Obchodní podmínky, Veřejnoprávní podklady, právní předpisy nebo příslušné ČSN předepisují provedení zkoušek, revizí, atestů a měření či zajištění prohlášení o shodě týkajících se Díla, je Zhotovitel povinen zajistit jejich úspěšné provedení před předáním Díla Objednateli.
103. Objednatel Dílo převezme za předpokladu, že provedení Díla odpovídá Smlouvě o dílo, Obchodním podmínkám, Veřejnoprávním podkladům, právním předpisům a příslušným ČSN, je dokončeno (plně funkční), a je prosté vad s výjimkou ojedinělých drobných vad, které samy o sobě ani ve spojení s jinými nebrání užívání Díla funkčně nebo esteticky, ani jeho užívání podstatným způsobem neomezuje.
104. Splnění podmínek pro předání Díla bude ověřeno v rámci přejímacího řízení. Zhotovitel je povinen písemně vyzvat Objednatele k převzetí Díla (zahájení přejímacího řízení). Přejímací řízení bude Objednatel zahájeno do 5 pracovních dnů po obdržení písemné výzvy Zhotovitele.
105. Objednatel je oprávněn přizvat k účasti v přejímacím řízení i jiné osoby, jejichž účast pokládá za nezbytnou.
106. O průběhu přejímacího řízení bude Zhotovitelem pořízen zápis s identifikací vad Díla, pokud budou v průběhu přejímacího řízení zjištěny. Zápis bude použit jako podklad pro zpracování Předávacího protokolu. Zpracování návrhu Předávacího protokolu zajistí Zhotovitel.
107. Předávací protokol obsahuje
- 107.1. výslovný souhlas Objednatele s převzetím Díla
 - 107.2. datum převzetí Díla,
 - 107.3. prohlášení Objednatele, zda přebírá Dílo bez výhrad, nebo s výhradami,
 - 107.4. soupis zjištěných vad nebránících řádnému užívání Díla,
 - 107.5. dohodnuté lhůty k odstranění zjištěných vad nebo jiná opatření (byla-li dohodnuta),
 - 107.6. soupis Dokladů předaných Zhotovitelem Objednateli.
108. Objednatel převezme Dílo bez výhrad, je-li v předávacím řízení zjištěno, že Dílo je prosté vad.
109. Převezme-li Objednatel Dílo s výhradami, postupují Smluvní strany dále obdobně dle ustanovení odstavců 138 - 152 Obchodních podmínek, přičemž pro odstranění vad platí doba sjednaná v Předávacím protokolu, jinak doba 15 dní od oboustranného podpisu Předávacího protokolu a za reklamaci se považuje identifikace vad uvedená v Předávacím protokolu podepsaném Objednatel.
110. V případě, že Objednatel Dílo nepřevzme, bude mezi Smluvními stranami sepsán záznam s uvedením důvodu nepřevzetí Díla a s uvedením stanovisek Smluvních stran. Zpracování záznamu zajistí Zhotovitel.
111. V případě nepřevzetí Díla Smluvní strany sjednají lhůtu pro odstranění zjištěných vad. Nebude-li vada odstraněna ve lhůtě sjednané, jinak do 15 dní, je Objednatel oprávněn zajistit odstranění vady jinou odborně způsobilou osobou na náklady Zhotovitele. Veškeré náklady vzniklé Objednateli v souvislosti s odstraněním vady způsobem dle předchozí věty je Zhotovitel povinen Objednateli uhradit. Zhotovitel je povinen ve stanovené lhůtě odstranit vady i v případě, kdy podle jeho názoru za vady neodpovídá. Náklady na odstranění v těchto sporných případech nese až do vyjasnění nebo do vyřešení rozporu Zhotovitel. Po odstranění vad vyzve Zhotovitel Objednatele k zahájení náhradního přejímacího řízení, které Objednatel zahájí bezodkladně, nejpozději do 2 pracovních dnů od obdržení výzvy Zhotovitele.

- 112. Podpisem Předávacího protokolu nebo záznamu o nepřevzetí Díla je přejímací řízení ukončeno.
- 113. Pro průběh náhradního přejímacího řízení se užijí ustanovení odstavců 103 - 112 Obchodních podmínek obdobně.
- 114. Připouští-li to povaha Předmětu díla, a není-li sjednán zkušební provoz, má Objednatel právo, aby byl Předmět díla před ním překontrolován nebo aby byly předvedeny jeho funkce.
- 115. Ustanovení §1921, §2112, §2605 odst. 2, §2606, §2609, §2618 a §2629 Občanského zákoníku se neužijí.

ČÁST 14 - VLASTNICKÉ PRÁVO A NEBEZPEČÍ ŠKODY

- 116. Vlastnické právo k Dílu náleží od počátku Objednateli.
- 117. Vlastnické právo k dodávkám materiálu a jiných hmotných movitých věcí nabývá Objednatel okamžikem jejich zapracování do Díla, učiněním součástí Díla nebo jakýmkoliv funkčním, estetickým či jiným spojením s Dílem.
- 118. Vlastnické právo k jakékoli dokumentaci vztahující se k Dílu, která není autorským dílem, nabývá Objednatel okamžikem jejího vyhotovení.
- 119. Je-li vlastníkem Díla nebo jeho části v souladu s §1083 a §1084 Občanského zákoníku vlastník pozemku, užijí se ustanovení odstavců 116 a 117 přiměřeně.
- 120. Nebezpečí škody na Díle nese Zhotovitel, na Objednatele přechází okamžikem oboustranného podpisu Předávacího protokolu. Pokud nebyly s Předmětem díla předány zároveň též všechny Doklady, nese Zhotovitel nebezpečí škody na dosud nepředaných Dokladech až do jejich převzetí Objednatelem.
- 121. Náklady nutné k odstranění škody na Díle vzniklé v době, kdy nebezpečí škody nese Zhotovitele, hradí Zhotovitel v plném rozsahu a tyto náklady nemají vliv na Cenu díla.
- 122. Škody na Díle vzniklé v době, kdy nebezpečí škody nese Zhotovitele, je povinen Zhotovitel odstranit v součinnosti s Objednatelem jako vlastníkem poškozené věci a dle jeho pokynů.
- 123. Ustanovení §2599 Občanského zákoníku se neužijí.

ČÁST 15 - VADY PLNĚNÍ A ZÁRUKA

- 124. Zhotovitel se zavazuje, že Dílo bude v okamžiku jeho převzetí Objednatelem vyhovovat všem požadavkům na dílo stanoveným Smlouvou o dílo, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN.
- 125. Zhotovitel se zavazuje, že Dílo bude vyhovovat též plnění nabídnutému Zhotovitelem v Nabídce.
- 126. Dílo musí být prosté všech faktických a právních vad. Plnění má právní vadu, pokud k němu uplatňuje právo třetí osoba.
- 127. Zhotovitel se zavazuje (poskytuje Objednateli záruku), že Dílo a veškeré jeho části si po celou dobu od okamžiku jeho převzetí Objednatelem, až do uplynutí Záruční doby zachová vlastnosti stanovené v odstavcích 124 - 126 Obchodních podmínek.
- 128. Záruční doba začíná běžet dnem převzetí Díla Objednatelem, nebo jeho poslední části, je-li Dílo dodáváno po částech, nebo ode dne úspěšného ukončení zkušebního provozu, je-li dle Smlouvy o dílo vyžadován a nastane-li okamžik úspěšného ukončení zkušebního provozu později než okamžik převzetí Díla, resp. jeho poslední části.
- 129. Dílo má vady (Zhotovitel plnil vadně), jestliže při převzetí Objednatelem nebo kdykoliv od převzetí Objednatelem do konce Záruční doby nebude mít vlastnosti stanovené v odstavcích 124 - 126 Obchodních podmínek.
- 130. Objednatel má práva z vadného plnění i v případě, jedná-li se o vadu, kterou musel s vynaložením obvyklé pozornosti poznat již při uzavření Smlouvy o dílo.
- 131. Objednatel nemá práva z vadného plnění, způsobila-li vadu po přechodu nebezpečí škody na věci na Objednatele vnější událost. To neplatí, způsobil-li vadu Zhotovitel nebo jakákoliv třetí osoba, jejímž prostřednictvím plnil své povinnosti vyplývající ze Smlouvy o dílo.

132. Zhotovitel neodpovídá za vady spočívající v opotřebení Předmětu díla, které je obvyklé u věcí stejného nebo obdobného druhu jako Předmět díla.
133. Zhotovitel odpovídá za vady spočívající v opotřebení Předmětu díla, ke kterému do konce Záruční doby vzhledem k požadavkům Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN na jakost a provedení Předmětu díla nemělo dojít.
134. Zhotovitel nenese odpovědnost za vady způsobené Objednatelem nebo třetími osobami, ledaže Objednatel nebo takové osoby postupovaly v souladu s Doklady nebo pokyny, které obdrželi od Zhotovitele.

ČÁST 16 - UPLATNĚNÍ PRÁV Z VADNÉHO PLNĚNÍ

135. Odpovídá-li Zhotovitel za vady Díla, má Objednatel práva z vadného plnění.
136. Objednatel je oprávněn vady reklamovat u Zhotovitele jakýmkoliv způsobem, preferovaná je písemná forma. Zhotovitel je povinen přijetí reklamace bez zbytečného odkladu písemně potvrdit. V reklamaci Objednatel uvede popis vady nebo uvede, jak se vada projevuje.
137. Vada je uplatněna včas, je-li písemná forma reklamace odeslána Zhotoviteli nejpozději v poslední den Záruční doby. Případně-li konec Záruční doby na sobotu, neděli nebo svátek, je vada včas uplatněna, je-li písemná forma reklamace odeslána Zhotoviteli nejbližší následující pracovní den.
138. Má-li Předmět díla vady, za které Zhotovitel odpovídá, má Objednatel právo
 - 138.1. na odstranění vady dodáním nového Předmětu díla nebo jeho části bez vady, pokud to není vzhledem k povaze vady zcela zřejmě nepřiměřené, nebo dodání chybějící části Předmětu díla,
 - 138.2. na odstranění vady opravou Předmětu díla nebo jeho části,
 - 138.3. na přiměřenou slevu z Ceny díla, nebo
 - 138.4. odstoupit od Smlouvy o dílo.
139. Objednatel je oprávněn požadovat odstranění vad dodáním nového Předmětu díla nebo jeho části bez vady, vyskytla-li se stejná vada po její opravě opětovně, nebo nemůže-li Objednatel řádně užívat Předmět díla nebo jeho část pro větší počet vad.
140. Objednatel je oprávněn nároky dle odstavce 138 kombinovat, je-li to vzhledem k okolnostem možné. Objednatel není oprávněn kombinovat nároky, které si navzájem odporují (např. dodání nové části Předmětu díla a zároveň slevy z Ceny díla na tutéž část Předmětu díla).
141. Objednatel sdělí Zhotoviteli volbu nároku z vady v reklamaci, nebo bez zbytečného odkladu po reklamaci. Provedenou volbu nemůže Objednatel změnit bez souhlasu Zhotovitele; to neplatí, žádal-li Objednatel opravu vady, která se ukáže jako neopravitelná.
142. Nesdělí-li Objednatel Zhotoviteli, jaké právo si zvolil ani bez zbytečného odkladu poté, co jej k tomu Zhotovitel vyzval, může Zhotovitel odstranit vady podle své volby opravou nebo dodáním nového Předmětu díla nebo jeho části; volba nesmí Objednateli způsobit nepřiměřené náklady.
143. Objednatel má nárok na náhradu nákladů účelně vynaložených v souvislosti s oznámením vad Zhotoviteli.

ČÁST 17 - PODMÍNKY ODSTRANĚNÍ VAD

144. Pokud Objednatel požaduje v reklamaci odstranění vady, je Zhotovitel povinen neprodleně po obdržení reklamace zahájit činnosti vedoucí k odstranění reklamované vady. Pokud Objednatel v reklamaci uvede, že se jedná o havárii, je Zhotovitel povinen zahájit odstraňování vady nejpozději do 48 hodin po obdržení reklamace.
145. Zhotovitel je povinen odstranit Objednatelem reklamovanou vadu nejpozději do 30 dnů ode dne oznámení vady Zhotoviteli. Jde-li o vadu označenou Objednatelem v reklamaci jako havarijní, je Zhotovitel povinen odstranit vadu nejpozději do 5 dnů.

146. Nezahájí-li Zhotovitel činnosti vedoucí k odstranění vady do 10 dnů od oznámení vady Zhotoviteli, nebo nebude-li vada odstraněna ve lhůtě dle předcházejícího odstavce, je Objednatel oprávněn
- 146.1. zajistit odstranění vady jinou odborně způsobilou právnickou nebo fyzickou osobou na účet Zhotovitele,
- 146.2. požadovat slevu z Ceny díla, nebo
- 146.3. od Smlouvy o dílo odstoupit.
147. Veškeré náklady vzniklé Objednateli v souvislosti s odstranění vady způsobem dle předchozího odstavce je Zhotovitel povinen Objednateli uhradit.
148. Zhotovitel je povinen odstranit vadu bez ohledu na to, zda je uplatnění vady oprávněné či nikoli. Prokáže-li se však kdykoli později, že uplatnění vady Objednatelem nebylo oprávněné, tj. že Zhotovitel za vadu neodpovídal, je Objednatel povinen uhradit Zhotoviteli veškeré jím účelně vynaložené náklady v souvislosti s odstraněním vady.
149. Objednatel je povinen poskytnout Zhotoviteli součinnost nezbytnou k odstranění vady.
150. Do odstranění vady nemusí Objednatel platit dosud nezaplacenou část Ceny díla a případnou příslušnou DPH odhadem přiměřeně odpovídající jeho právu na slevu.
151. Při dodání nového Předmětu díla nebo jeho části vrátí Objednatel Zhotoviteli na náklady Zhotovitele Předmět díla nebo jeho část původně dodanou.
152. Týká-li se vada Dokladů nebo jiného plnění poskytnutého Zhotovitelem dle Smlouvy o dílo než Předmětu díla, užijí se ustanovení odstavců 135 – 151 obdobně.
153. Ustanovení §1917–1924, §2099–2101, §2103 – 2117, §2165 – 2172, §2618 a §2629 Občanského zákoníku se neužijí.

ČÁST 18 - POJIŠTĚNÍ

154. Ustanovení této části se užijí v případě, že ze Smlouvy o dílo vyplývá, že Zhotovitel je povinen být pojištěn pro případ odpovědnosti za škodu způsobenou při výkonu činnosti.
155. Zhotovitel je povinen mít ode dne zahájení provádění Díla, nejpozději však do 15 dnů od uzavření Smlouvy o dílo, až do uplynutí Záruční doby uzavřenou pojistnou smlouvu o pojištění odpovědnosti za škodu způsobenou Zhotovitelem při výkonu činnosti třetím osobám s limitem pojistného plnění pro 1 pojistnou událost ve výši odpovídající Ceně díla.
156. Zhotovitel je povinen předložit Objednateli uzavřenou pojistnou smlouvu dle této části nebo odpovídající pojistku nejpozději do 15 dnů ode dne uzavření Smlouvy o dílo a dále kdykoli v průběhu provádění Díla nebo trvání Záruční doby do 10 dnů ode dne, kdy k tomu byl Objednatelem vyzván. V případě změn v pojištění je Zhotovitel povinen bezodkladně tyto změny oznámit Objednateli a předložit dokumenty dokládající tyto změny.
157. Zhotovitel se zavazuje, že všichni poddodavatelé, kteří se budou podílet na provedení Díla, budou nejméně po dobu provádění poddodávky pojištěni pro případ škody způsobené poddodavatelem při výkonu činnosti třetím osobám s limitem pojistného plnění pro 1 pojistnou událost minimálně ve výši odpovídající ceně poddodávky.
158. Porušení jakékoli povinnosti Zhotovitele dle této části je podstatným porušením Smlouvy o dílo.
159. Náklady na pojištění nese Zhotovitel, jsou zahrnuty v Ceně díla.

ČÁST 19 - DUŠEVNÍ VLASTNICTVÍ

160. Zhotovitel je povinen při provádění Díla postupovat tak, aby při provádění Díla ani následným užíváním Díla Objednatelem nedošlo k porušení práv duševního vlastnictví. Bude-li v souvislosti s Dílem, jakkoliv dotčeno právo k duševnímu vlastnictví, je Zhotovitel povinen upravit veškeré právní vztahy s osobami, kterým taková práva náleží nebo jež jsou oprávněny je vykonávat, tak, aby zamezil vznášení jakýchkoli oprávněných nároků těchto osob ve vztahu k Objednateli.
161. Zhotovitel tímto poskytuje Objednateli oprávnění k výkonu práva duševního vlastnictví (licenci nebo podlicenci) ke všem plněním poskytnutým Objednateli při provádění Díla,

161. které jsou nebo budou předmětem duševního vlastnictví a ke kterým je oprávněn takové oprávnění poskytnout. Oprávnění Zhotovitel poskytuje
- 161.1. bezúplatně,
 - 161.2. jako nevýhradní,
 - 161.3. z hlediska časového a územního v rozsahu neomezeném,
 - 161.4. z hlediska věcného rozsahu (způsobu užití) tak, že opravňuje Objednatele ke všem známým způsobům užití,
 - 161.5. bez množstevního omezení.
162. Objednatel není povinen oprávnění využít.
163. Objednatel je oprávněn oprávnění tvořící součást licence nebo podlicence poskytnout nebo též postoupit třetí osobě zcela nebo zčásti.
164. Zhotovitel se zavazuje, že na žádost Objednatele autor nebo autoři autorského díla, jež je součástí nebo příslušenstvím Díla, udělí Objednateli bez zbytečného odkladu bezúplatně právo
- 164.1. upravit či jinak změnit označení autora,
 - 164.2. autorské dílo nebo jeho název upravit či jinak měnit,
 - 164.3. autorské dílo s jakýmkoliv jiným autorským dílem spojit či zařadit do díla souborného.
165. Žádný výsledek činnosti provedené na základě Smlouvy o dílo nebo v souvislosti s ní, který je předmětem duševního vlastnictví, není Zhotovitel oprávněn bez předchozího písemného svolení Objednatele užit k jiným účelům, než je provedení Díla, zejména je nesmí poskytnout třetím osobám.

ČÁST 20 - SANKCE

166. Poruší-li Zhotovitel povinnost provést Dílo ve sjednané době, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 0,5 % z Ceny díla za každý den prodlení.
167. Poruší-li Objednatel povinnost zaplatit Cenu díla ve sjednané době, je povinen uhradit Zhotoviteli zákonný úrok z prodlení ve výši dle právních předpisů.
168. Poruší-li Zhotovitel povinnost odstranit vadu Díla ve sjednané době, je povinen uhradit Objednateli smluvní pokutu ve výši 0,5 % z Ceny díla za každý den prodlení až do odstranění vady. Jde-li o vadu, kterou Objednatel označil v reklamaci jako havárii, je Zhotovitel povinen uhradit smluvní pokutu ve dvojnásobné výši.
169. Poruší-li Zhotovitel povinnost nepostoupit žádnou svou pohledávku za Objednatelem vyplývající ze Smlouvy o dílo a/nebo poruší zákaz zřídit zástavní právo k pohledávce, byť by takové postoupení a/nebo zřízení zástavního práva bylo neplatné či neúčinné, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 10 % z nominální hodnoty postoupené a/nebo zastavené pohledávky, včetně hodnoty případného příslušenství ke dni účinnosti postoupení vůči postupníkovi.
170. Poruší-li Zhotovitel jakékoliv jiné povinnosti vyplývající ze Smlouvy o dílo, Obchodních podmínek nebo Veřejnoprávních podkladů než povinnosti, na které se vztahuje smluvní pokuta dle této části, je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 5% z Ceny díla za každý jednotlivý případ porušení povinnosti.
171. Poruší-li Zhotovitel nebo osoba, kterou Zhotovitel používá při provádění díla jakoukoliv povinnost stanovenou Směrnicí SŽDC č. 120 Dodržování zákazu kouření, požívání alkoholických nápojů a užívání jiných návykových látek, č.j. 36503/2017-SŽDC-GR-O10 ze dne 3.11.2017, účinnou od 7.1.1.2017 v rámci Objednatelem prováděné kontroly na základě výše uvedené směrnice je Objednatel oprávněn na základě posouzení souvisejících okolností, uplatnit vůči Zhotoviteli sankci ve výši 5 000,- Kč za každý jednotlivý případ.
172. Zaplacení smluvní pokuty nezbujuje Zhotovitele povinnosti splnit dluh smluvní pokutou utvrzený.
173. Objednatel je oprávněn požadovat náhradu škody a nemajetkové újmy způsobené porušením povinnosti, na kterou se vztahuje smluvní pokuta, v plné výši.

ČÁST 21 - OBECNÁ ODPOVĚDNOST ZHOTOVITELE

174. Zhotovitel je povinen po dobu plnění povinností ze Smlouvy o dílo chránit majetek Objednatele i třetích osob před jeho poškozením, znehodnocením, zničením a ztrátou a postupovat tak, aby neomezoval práva osob nad míru nezbytnou k provádění Díla.
175. Způsobí-li Zhotovitel v souvislosti s Dílem nebo porušením svých povinností vyplývajících ze Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN jakoukoli újmu Objednateli nebo třetím osobám, je povinen nahradit Objednateli škodu a nemajetkovou újmu, včetně případných sankcí udělených Objednateli orgány státní správy, jejichž příčinou bylo porušení smluvních povinností Zhotovitele, a jde-li o újmu způsobenou třetím osobám, je povinen způsobenou újmu na vlastní náklady bezodkladně odčinit.
176. Újmou se pro účely Obchodních podmínek rozumí zejm. jakékoliv poškození, znehodnocení, či znečištění věcí nebo prostor nebo jejich jiná nežádoucí změna a jakékoliv neoprávněné omezení práv Objednatele nebo třetích osob.
177. Zhotovitel odpovídá za jakékoli porušení svých povinností stanovených Smlouvou o dílo, Obchodními podmínkami, Veřejnoprávními podklady, právními předpisy a příslušnými ČSN a je povinen uhradit veškeré pokuty udělené mu příslušnými orgány státní správy v souvislosti s prováděním Díla ze svého, ledaže mu byla pokuta udělena v souvislosti s respektováním příkazu Objednatele, proti kterému uplatnil písemnou výhradu a na jehož splnění Objednatel trval anebo v souvislosti s užitím Objednatелеm opatřené věci, na jejíž nevhodnost Objednatele písemně upozornil a Objednatel na jejím užití trval.
178. Povinnosti k náhradě újmy způsobené porušením svých povinností ze Smlouvy o dílo, Obchodních podmínek, Veřejnoprávních podkladů, právních předpisů a příslušných ČSN se Zhotovitel vůči Objednateli zproští, prokáže-li, že mu ve splnění povinnosti zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá z osobních poměrů Zhotovitele nebo vzniklá až v době, kdy byl Zhotovitel s plněním povinnosti v prodlení, ani překážka, kterou byl Zhotovitel povinen překonat, jej však povinnosti k náhradě nezproští.

ČÁST 22 - Odstoupení od smlouvy o dílo

179. Poruší-li Smluvní strana Smlouvu o dílo podstatným způsobem, může druhá Smluvní strana písemnou formou od Smlouvy o dílo odstoupit.
180. Podstatné je takové porušení povinnosti, o němž Smluvní strana porušující Smlouvu o dílo již při uzavření Smlouvy o dílo věděla nebo musela vědět, že by druhá Smluvní strana Smlouvu o dílo neuzavřela, pokud by toto porušení předvíдалa, nebo je-li porušení povinnosti ve Smlouvě o dílo nebo v Obchodních podmínkách jako podstatné označeno; v ostatních případech se má za to, že porušení podstatné není.
181. Podstatným porušením Smlouvy o dílo je též prodlení Zhotovitele a Objednatele s plněním povinností vyplývajících Zhotoviteli a Objednateli ze Smlouvy o dílo o více než 30 dní.
182. Objednatel je oprávněn od Smlouvy o dílo odstoupit též
- 182.1. z důvodů uvedených v části Předání a převzetí Díla (viz ČÁST 13 - Obchodních podmínek),
 - 182.2. nabylo-li právní moci rozhodnutí o nařízení exekuce vůči Zhotoviteli jako povinnému,
 - 182.3. ocitne-li se Zhotovitel ve stavu úpadku nebo hrozícího úpadku,
 - 182.4. jestliže Zhotovitel nebo jeho poddodavatel, nebo z jejich pokynu jakákoliv osoba, nabídne nebo poskytne jakékoliv osobě úplatek nebo jiný majetkový či jiný prospěch za účelem získání neoprávněného prospěchu nebo výhody v souvislosti s Dílem nebo jeho prováděním,
 - 182.5. uvedl-li Zhotovitel v Nabídce informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek řízení,
 - 182.6. stanoví-li tak Smlouvy o dílo.

183. Smluvní strana může od Smlouvy o dílo odstoupit, pokud z chování druhé Smluvní strany nepochybně vyplývá, že poruší Smlouvu o dílo podstatným způsobem, a nedá-li na výzvu oprávněné Smluvní strany přiměřenou jistotu.
184. Jakmile Smluvní strana oprávněná odstoupit od Smlouvy o dílo oznámí druhé Smluvní straně, že od Smlouvy o dílo odstupuje, nebo že na Smlouvě o dílo setrvává, nemůže volbu již sama změnit.
185. Zakládá-li prodlení Smluvní strany nepodstatné porušení její povinnosti ze Smlouvy o dílo, může druhá Smluvní strana od Smlouvy o dílo odstoupit poté, co prodlévající Smluvní strana svoji povinnost nesplní ani v dodatečně přiměřené lhůtě, kterou jí druhá Smluvní strana poskytla výslovně nebo mlčky.
186. Oznámí-li Smluvní strana Smluvní straně prodlévající, že jí určuje dodatečnou lhůtu k plnění a že jí lhůtu již neprodlouží, platí, že marným uplynutím této lhůty od Smlouvy o dílo odstoupila.
187. Poskytla-li Smluvní strana Smluvní straně prodlévající nepřiměřeně krátkou dodatečnou lhůtu k plnění a odstoupí-li od Smlouvy o dílo po jejím uplynutí, nastávají účinky odstoupení teprve po marném uplynutí doby, která měla být prodlévající Smluvní straně poskytnuta jako přiměřená. To platí i tehdy, odstoupila-li Smluvní strana od Smlouvy o dílo, aniž by prodlévající Smluvní straně dodatečnou lhůtu k plnění poskytla.
188. Plnil-li Zhotovitel zčásti, může Smluvní strana od Smlouvy o dílo odstoupit jen ohledně nesplněného zbytku plnění. Nemá-li však částečné plnění pro Objednatele význam, může Objednatel od Smlouvy o dílo odstoupit ohledně celého plnění. Odstoupil-li od nesplněného zbytku plnění Zhotovitel, je Objednatel oprávněn odstoupit od splněné části Smlouvy o dílo, nemá-li částečné plnění pro Objednatele význam.
189. Zavazuje-li Smlouva o dílo Zhotovitele k opakované činnosti nebo k postupnému dílčímu plnění, může Objednatel od Smlouvy o dílo odstoupit jen s účinky do budoucna. To neplatí, nemají-li již přijatá dílčí plnění sama o sobě pro Objednatele význam.
190. Smluvní strany se dohodly, že dojde-li k odstoupení od Smlouvy o dílo jen ohledně nesplněného zbytku plnění, užijí se na splněnou část plnění obdobně všechna ustanovení Smlouvy o dílo a Obchodních podmínek týkající se předání a převzetí Díla, přičemž přejímací řízení Smluvní strany zahájí nejpozději do 3 pracovních dnů ode dne odstoupení od Smlouvy o dílo, a dále všechna ustanovení Smlouvy o dílo a Obchodních podmínek o právech a povinnostech Smluvních stran, které jsou Smluvní strany povinny plnit v době ode dne převzetí Díla Objednatelem, tedy zejm. ustanovení o vadách Díla.
191. Ustanovení §1977, §2002–2003 Občanského zákoníku se neužijí.

ČÁST 23 - OSTATNÍ UJEDNÁNÍ

Částečné plnění

192. Ustanovení Smlouvy o dílo a Obchodních podmínek platí obdobně též pro části Díla, provádí-li Zhotovitel Dílo v souladu se Smlouvou o dílo po částech, není-li uvedeno jinak.

Postoupení, započtení

193. Zhotovitel není oprávněn postoupit žádnou svou pohledávku za Objednatelem vyplývající ze Smlouvy o dílo nebo vzniklou v souvislosti se Smlouvou o dílo.
194. K pohledávce za Objednatelem vyplývající se Smlouvy o dílo nebo vzniklé v souvislosti se Smlouvou o dílo nesmí být zřízeno zástavní právo.
195. Zhotovitel není oprávněn provést jednostranné započtení žádné své pohledávky za Objednatelem vyplývající ze Smlouvy o dílo nebo vzniklé v souvislosti se Smlouvou o dílo na jakoukoliv pohledávku Objednatele za Zhotovitelem.
196. Objednatel je oprávněn provést jednostranné započtení jakékoliv své splatné i nesplatné pohledávky za Zhotovitelem vyplývající ze Smlouvy o dílo nebo vzniklé v souvislosti se Smlouvou o dílo (zejm. smluvní pokutu) na jakoukoliv splatnou či nesplatnou pohledávku Zhotovitele za Objednatelem.

Mlčenlivost

197. Zhotovitel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které jsou obsaženy ve Smlouvě o dílo a dále o všech skutečnostech a informacích, které mu byly v souvislosti se Smlouvou o dílo nebo jejím plněním, jakkoliv zpřístupněny, předány

či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi Zhotovitel seznámil, prokazatelně veřejně přístupné, nebo těch, které se bez zavinění Zhotovitele veřejně přístupnými stanou. Zhotovitel nesmí takové skutečnosti a informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch Objednatele. Povinnosti dle tohoto odstavce je Zhotovitel povinen zachovávat i po zániku závazku ze Smlouvy o dílo, vyjma případů, kdy se takové skutečnosti a informace stanou prokazatelně veřejně přístupné bez zavinění Zhotovitele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je Zhotovitel povinen zveřejnit takové skutečnosti nebo informace na základě povinnosti uložené mu právním předpisem nebo rozhodnutím orgánu veřejné moci.

Poskytování informací

198. Vzhledem k veřejnoprávnímu charakteru Objednatele Zhotovitel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním Smlouvy o dílo včetně Obchodních podmínek v rozsahu a za podmínek vyplývajících z příslušných právních předpisů.

Kontrola

199. Zhotovitel si je vědom, že je ve smyslu §2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, povinen spolupůsobit při výkonu finanční kontroly a zavazuje se finanční kontrolu strpět.
200. Je-li Dílo z jakékoliv části financováno z prostředků Evropské unie, je Zhotovitel povinen
- 200.1. strpět veškeré kontroly vyplývající z režimu financování Díla z prostředků Evropské unie,
- 200.2. poskytnout při takových kontrolách veškerou nezbytnou součinnost,
- 200.3. archivovat veškerou dokumentaci týkající se Smlouvy o dílo po dobu stanovenou pravidly, jimiž se řídí financování Díla z prostředků Evropské unie.

Jazyk

201. Ve všech záležitostech souvisejících se Smlouvou o dílo budou zástupci Smluvních stran komunikovat v českém jazyce. Všichni zástupci musí plynňě český jazyk ovládat. Jestliže český jazyk plynňě neovládají, jsou povinni na náklady své Smluvní strany zajistit, aby byl po celou dobu vzájemné osobní komunikace k dispozici kvalifikovaný tlumočník.

Forma, označení času

202. Písemnou formou (podobou) se rozumí listina podepsaná oprávněnou osobou Smluvní strany nebo email podepsaný zaručeným elektronickým podpisem oprávněné osoby Smluvní strany.
203. Je-li ve Smlouvě o dílo nebo Obchodních podmínkách uvedena lhůta nebo doba počítané podle dnů, měsíců nebo let, rozumí se tím vždy kalendářní den, měsíc nebo rok, není-li uvedeno jinak.

Reference

204. Zhotovitel je oprávněn uvádět Dílo a jméno Objednatele jako referenci na svou činnost pouze s předchozím písemným souhlasem Objednatele.

Salvatorní klauzule

205. Je-li nebo stane-li se některé oddělitelné ustanovení Smlouvy o dílo nebo Obchodních podmínek neplatné, neúčinné či nevymahatelné, nedotýká se tato skutečnost ostatních ustanovení. Smluvní strany se zavazují nahradit takové ustanovení jiným ustanovením, které svým obsahem a smyslem bude nejvíce odpovídat obsahu a smyslu ustanovení nahrazovaného.

Příloha č. 7 zadávací dokumentace

Čestné prohlášení o splnění technické kvalifikace – seznam významných zakázek

Účastník:

Obchodní firma/jméno

Sídlo/místo podnikání

IČO

Zastoupen

.....

.....

.....

.....

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Log management a SIEM**“, č.j. **61441/2023-SŽ-GŘ-08**, tímto čestně prohlašuje, že za poslední 3 roky před zahájením zadávacího řízení realizoval alespoň 2 významné zakázky definované v čl. 13.1.1 písm. a) zadávací dokumentace.

Objednatel významné zakázky Název, IČO, sídlo, místo podnikání, kontakt k ověření realizované významné zakázky (telefonní a e-mailový kontakt na kontaktní osobu)	Název a předmět plnění významné zakázky (pokud významná zakázka nebyla v době zahájení zadávacího řízení dokončena, uveďte dodavatel i stupeň dokončení v souladu s čl. 13.1.2 zadávací dokumentace)	Celkový finanční objem významné zakázky	Doba realizace (datum od-do, v rámci 3 kalendářních let nazpět před zahájením zadávacího řízení)

V dne

Příloha č. 8 zadávací dokumentace

Seznam členů realizačního týmu

Účastník:

Obchodní firma/jméno

Sídlo/místo podnikání

IČO

Zastoupen

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Log management a SIEM**“, č.j. **61441/2023-SŽ-GR-O8**, tímto níže předkládá seznam členů realizačního týmu, kteří se budou na plnění předmětu veřejné zakázky podílet:

Pozice člena realizačního týmu	Jméno a příjmení	Praxe (dle pozice člena realizačního týmu v souladu s čl. 13.2 zadávací dokumentace)	Certifikát (pokud je u člena realizačního týmu vyžadován dle čl. 13.2 zadávací dokumentace)	Zkušenost (pokud je u člena realizačního týmu vyžadována dle čl. 13.2 zadávací dokumentace)	Vztah k dodavateli (např. zaměstnanec, OSVČ...)
Bezpečnostní architekt SIEM architekt					
Administrátor SIEM Administrátor SIEM					
Administrátor SIEM					

Projektový manažer					
-------------------------------	--	--	--	--	--

V dne

—

—

Nabídková cena

Účastník vyplní **ve sloupci E** ("Jednotková cena (bez DPH, v CZK)") jednotkovou cenu **v Kč bez DPH** za každou část (etapu) dodávky řešení: E1, E2, E3, E4, E5 a E6 v řádcích 11 až 18.

V případě, že formulář obsahuje červeně zbarvenou celkovou nabídkovou cenu, nabídka pravděpodobně obsahuje nesprávně vyplněné údaje, které mohou vést až k vyloučení účastníka ze zadávacího řízení.

Maximální a nepřekročitelná cena veřejné zakázky (nesmí být překročena v řádku 19): **95 000 000 CZK**

Etap	Část dodávky	Odkaz na kapitulu TS	Jednotková cena (bez DPH, v CZK)	Počet jednotek	jedn.	Nabídková cena (bez DPH, v CZK)
E1	Před-implementační analýza, Implementační služby (napojení určených zdrojů logů pro Etapu 1)	4.1.1;4.1.2;4.1.3		1	-	0,00 CZK
E1	Licence, údržba licencí a technická podpora výrobce na 60 měsíců , nebo supskripce licencí včetně údržby a technické podpory na 60 měsíců (celková cena za výčet licencí uvedených v Příloze č. 20 zadávací dokumentace "Log management a SIEM dotazník", záložka Licence)	2.4		1	-	0,00 CZK
E1	Hardwarové prostředky, dodávané nad rámec specifikovaných Požadavků na služby Platformy SŽ, technická podpora výrobce HW na 60 měsíců, údržba a technická podpora HW dodavatele na 60 měsíců*	2.4.13		1	-	0,00 CZK
E2	Implementační služby (napojení určených zdrojů logů pro Etapu 2)	4.1.3		1	-	0,00 CZK
E3	Tvorba a optimalizace bezpečnostní / detekční politiky řešení, Školení	4.1.4;4.1.5		1	-	0,00 CZK
E4	Implementační služby (napojení určených zdrojů logů pro Etapu 4)	4.1.3		1	-	0,00 CZK
E5	Technická podpora servisního týmu SŽ, údržba řešení	4.2.1; 4.2.2		60	měsíc	0,00 CZK
E6	Konzultace a rozvojové aktivity	4.2.3		250	MD**	0,00 CZK
	NABÍDKOVÁ CENA CELKEM		0 CZK			0,00 CZK

**MD = člověkodenní

* Tuto položku může dodavatel ocenit i hodnotou 0, a to v případě, že z jeho strany nebudou dodávány žádné další hardwarové prostředky nad rámec specifikovaných Požadavků na služby Platformy SŽ (viz čl. 18.3 zadávací dokumentace).

Příloha č. 10 zadávací dokumentace

DOHODA O OCHRANĚ DŮVĚRNÝCH INFORMACÍ

k veřejné zakázce:

„Log management a SIEM“

Smluvní strany:

Správa železnic, státní organizace

se sídlem: Dlážděná 1003/7, 110 00 Praha 1

IČO: 70994234, DIČ: CZ70994234

zastoupená: **Ing. David Miklas**

(dále jen „**Zadavatel**“)

a

[DOPLNÍ DODAVATEL]

se sídlem: [DOPLNÍ DODAVATEL]

IČO: [DOPLNÍ DODAVATEL], DIČ: [DOPLNÍ DODAVATEL]

společnost zapsaná v obchodním rejstříku vedeném [DOPLNÍ DODAVATEL] soudem v [DOPLNÍ DODAVATEL]

oddíl [DOPLNÍ DODAVATEL], vložka [DOPLNÍ DODAVATEL]

zastoupená: [DOPLNÍ DODAVATEL]

(dále jen „**Dodavatel**“)

(společně také jako „**Strany**“)

dnešního dne uzavřely tuto dohodu v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, v platném znění (dále jen „**Občanský zákoník**“)

(dále jen „**Dohoda**“)

1. ÚČEL DOHODY

- 1.1 Zadavatel zadává nadlimitní sektorovou veřejnou zakázku s názvem **“Log management a SIEM”** (dále jen **„Veřejná zakázka“**) podle ustanovení § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen **„ZZVZ“**). Dodavatel s úmyslem účastnit se zadávacího řízení na zadání Veřejné zakázky požaduje vydání částí zadávací dokumentace uvedených v Příloze č. 1 této Dohody, které obsahují informace, jež Zadavatel považuje za důvěrné a vyžaduje jejich ochranu (dále jen **„Důvěrné informace“**). Z tohoto důvodu uzavírají Strany tuto Dohodu, která upravuje pravidla pro nakládání s Důvěrnými informacemi převzatými Dodavatelem.

2. PŘEDMĚT DOHODY

- 2.1 Veškeré informace uvedené v Příloze č. 1 této Dohody, jsou považovány za Důvěrné informace, jejichž použití podléhá této Dohodě.
- 2.2 Dodavatel se zavazuje, že Důvěrné informace dle této Dohody použije pouze způsobem a k účelu v této Dohodě stanoveným.

3. UŽITÍ DŮVĚRNÝCH INFORMACÍ

- 3.1 Dodavatel je oprávněn Důvěrné informace užít jen pro účely své účasti v zadávacím řízení na zadání Veřejné zakázky a dále při jejím případném plnění.
- 3.2 Dodavatel se zavazuje zachovat důvěrnost Důvěrných informací a nezpřístupnit je žádné třetí osobě.
- 3.3 Svým zaměstnancům a orgánům je Dodavatel oprávněn Důvěrné informace zpřístupnit jen v rozsahu, v jakém je pro danou osobu nezbytně nutné se s Důvěrnými informacemi seznámit pro účely účasti Dodavatele v zadávacím řízení na zadání Veřejné zakázky nebo případně jejího plnění. Tyto osoby musí být poučeny o důvěrném charakteru předávaných informací a v rozsahu odpovídajícím této Dohodě zavázány k mlčenlivosti.
- 3.4 Dodavatel je oprávněn zpřístupnit Důvěrné informace jiným třetím osobám jen s předchozím písemným souhlasem Zadavatele, anebo při splnění podmínek uvedených v článku 4 této Dohody.
- 3.5 Po doručení této podepsané Dohody ze strany Dodavatele Zadavateli prostřednictvím elektronického nástroje E-ZAK bude ve lhůtě dle § 96 odst. 2 ZZVZ předán Dodavateli přístupový údaj k Důvěrným informacím – heslo k neveřejné části zadávací dokumentace k Veřejné zakázce, a to formou SMS zprávy zaslané na číslo určené Dodavatelem. Obdrží-li Dodavatel heslo, potvrdí tuto skutečnost odesláním takové zprávy zpět na číslo, z kterého heslo obdržel. Neobdrží-li Dodavatel předmětné heslo ve lhůtě 48 hodin od odeslání podepsané Dohody Zadavateli, obrátí se na Zadavatele prostřednictvím elektronického nástroje E-ZAK s tím, že heslo neobdržel. Nebude-li z jakéhokoli důvodu technicky možné heslo předat předvídaným způsobem, mohou Smluvní strany dohodnout jiný způsob předání hesla, ten však jasně zdokumentují a provedou tak, aby nedošlo k narušení zásad zadávání Veřejné zakázky ve smyslu § 6 ZZVZ.
- 3.6 Dodavatel určuje jako osobu pro obdržení a správu hesla k neveřejné části zadávací dokumentace osobu: **JMÉNO A PŘÍJMENÍ DOPLNÍ DODAVATEL**. Tato osoba je

oprávněna jednat za Dodavatele. Telefonní číslo, na které má být heslo zasláno je: **DOPLNÍ DODAVATEL.** Dodavatel se zavazuje, že uvedené telefonní číslo je telefonním číslem osoby uvedené v tomto článku Dohody.

4. PODDODAVATELÉ

- 4.1 Pokud Dodavatel zvažuje spolupracovat při přípravě nabídky na realizaci Veřejně zakázky a/nebo při eventuálním plnění Veřejné zakázky Dodavatelem se třetími osobami (dále jen „**Poddodavatelé**“), zavazuje se sdílet s těmito osobami Důvěrné informace jen v souladu s tímto článkem 4 této Dohody.
- 4.2 Za Poddodavatele se považuje jakákoliv třetí osoba spolupracující s Dodavatelem dle odst. 4.1 této Dohody bez ohledu na to, zda:
- 4.2.1 spolupráce probíhá v rámci konsorcia Dodavatele a takovéto třetí osoby, jehož členové odpovídají Zadavateli společně a nerozdílně, nebo
- 4.2.2 spolupráce je založena na poddodavatelském vztahu takovéto třetí osoby vůči Dodavateli, nebo
- 4.2.3 spolupráce je založena na poddodavatelském vztahu Dodavatele vůči takovéto třetí osobě, nebo
- 4.2.4 Dodavatel a třetí osoba zvolili eventuální jinou formu spolupráce.
- 4.3 Za Poddodavatele se považují i zajišťovny a další pojistitelé poskytující Dodavateli zajištění pro účely plnění veřejné zakázky.
- 4.4 Dodavatel je oprávněn sdílet Důvěrné informace s Poddodavateli pouze za předpokladu, že jsou vázáni mlčenlivostí minimálně v rozsahu dle této Dohody.

5. SPLNĚNÍ ÚČELU DOHODY

- 5.1 Dodavatel se zavazuje, že Důvěrné informace, přístupové údaje k Důvěrným informacím a rovněž jakékoliv kopie Důvěrných informací, které v souvislosti s plněním předmětu a účelu této Dohody pořídil, znehodnotí tak, že informace nebudou dále zobrazitelné, použitelné ani obnovitelné, a to bezodkladně po:
- (i) uplynutí lhůty pro podání nabídek do zadávacího řízení na zadání Veřejné zakázky, nepodal-li nabídku před jejím uplynutím;
- (ii) skončení účasti Dodavatele v zadávacím řízení na zadání Veřejné zakázky nebo ukončení zadávacího řízení, pokud s ním nebyla uzavřena smlouva na plnění veřejné zakázky;
- (iii) nebo po doručení písemné výzvy Zadavatele.

6. PORUŠENÍ POVINNOSTÍ

- 6.1 Poruší-li Poddodavatel dohodu uzavřenou s Dodavatelem nebo Zadavatelem na základě odst. 4.4 této Dohody a Zadavateli v důsledku toho vznikne škoda, Dodavatel za takto vzniklou škodu odpovídá.
- 6.2 Za každé jednotlivé porušení povinnosti Dodavatele uvedené v článku 3 této Dohody nebo povinnosti dle odst. 4.4 této Dohody, má Zadavatel právo požadovat zaplacení smluvní pokuty ze strany Dodavatele ve výši 500.000 Kč (slovy: pět set tisíc korun českých). Za porušení těchto povinností Dodavatele se nepovažuje nakládání

s Důvěrnými informacemi, které jsou veřejně známy nebo se staly veřejně známými bez porušení této Dohody, a dále poskytnutí Důvěrných informací na základě právních předpisů či vykonatelného rozhodnutí soudu nebo jiného orgánu veřejné moci.

- 6.3 Povinnost Dodavatele zaplatit smluvní pokutu dle této Dohody se nedotýká nároku Zadavatele na náhradu škody způsobené porušením povinnosti, které ke vzniku nároku na smluvní pokutu vedlo, a to v plné výši.

7. ZÁVĚREČNÁ USTANOVENÍ

- 7.1 Povinnost chránit Důvěrné informace zavazuje Dodavatele bez ohledu na případné ukončení této Dohody po dobu pěti (5) let od uzavření této Dohody. Ustanovení o odpovědnosti a smluvních pokutách se uplatní také v případě porušení povinnosti chránit Důvěrné informace dle předchozí věty.
- 7.2 Tuto Dohodu je možné měnit pouze písemnou dohodou Stran ve formě číslovaných dodatků k této Dohodě, podepsaných za každou Stranu osobou nebo osobami oprávněnými zastupovat tuto Stranu.
- 7.3 Veškerá práva a povinnosti vyplývající z této Dohody přecházejí, pokud to povaha těchto práv a povinností nevylučuje, na právní nástupce Stran.
- 7.4 Nedílnou součástí Dohody tvoří tyto přílohy:
Příloha č. 1: Specifikace Důvěrných informací
- 7.5 Tato Dohoda je vyhotovena v elektronické podobě, přičemž obě Strany obdrží její elektronický originál opatřený elektronickými podpisy. V případě, že tato Dohoda z jakéhokoli důvodu nebude vyhotovena v elektronické podobě, bude sepsána ve třech (3) stejnopisech, z nichž Zadavatel obdrží dvě (2) vyhotovení a Dodavatel obdrží jedno (1) Vyhotovení.

Strany prohlašují, že si tuto Dohodu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

Za Zadavatele

V Praze, dne _____

.....
.....

Správa železnic, státní organizace

Ing. David Miklas

ředitel Správy železniční telematiky

Za Dodavatele

V [DOPLNÍ DODAVATEL], dne [DOPLNÍ
DODAVATEL]

.....
.....

[DOPLNÍ DODAVATEL]

[DOPLNÍ DODAVATEL]

Příloha č. 1 Dohody o ochraně důvěrných informací**Specifikace Důvěrných informací**

Zadavatel poskytuje Dodavateli níže uvedené Důvěrné informace. Heslo k zpřístupnění těchto dokumentů bude po podpisu této Dohody předáno Dodavateli prostřednictvím SMS na telefonní číslo jím určené v Dohodě.

Seznam Důvěrných informací:

1. Příloha č. 2 zadávací dokumentace – Analýza prostředí – architektura prostředí SŽ
2. Příloha č. 3 zadávací dokumentace – Analýza prostředí – popis prostředí sítě UAS
3. Příloha č. 18 zadávací dokumentace – Interní předpis Zadavatele „Provozní politika prvků v působnosti systému řízení bezpečnosti informací“
4. Příloha č. 21 zadávací dokumentace – Zdroje logů 2023 – 05

Příloha č. 11 zadávací dokumentace

Čestné prohlášení účastníka

Účastník:

Obchodní firma/jméno

.....

Sídlo/místo podnikání

.....

IČO

.....

Zastoupen

.....

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Log management a SIEM**“, č.j. **61441/2023-SŽ-GR-08**, tímto čestně prohlašuje, že v souvislosti se zadávanou veřejnou zakázkou neuzavřel a neuzavře s jinými osobami zakázanou dohodu ve smyslu zákona č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů.

Účastník si je vědom všech právních důsledků, které pro něj mohou vyplývat z nepravdivosti zde uvedených údajů a skutečností.

V dne

Příloha č. 12 zadávací dokumentace – **Účastník předloží pouze v případě postupu dle čl. 25 zadávací dokumentace**

Čestné prohlášení

v souvislosti s ustanovením § 3 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „ZRS“)

Účastník:

Obchodní firma/jméno

Sídlo/místo podnikání

IČO

Zastoupen

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Log management a SIEM**“, č.j. **61441/2023-SŽ-GR-08**, tímto čestně prohlašuje, že dále uvedené údaje a další skutečnosti uvedené či jinak řádně označené ve smlouvě na plnění předmětu veřejné zakázky, jež je součástí jeho nabídky (dále jen „**smlouva**“), považuje účastník za obchodní tajemství ve smyslu ustanovení § 504 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**obchodní tajemství**“ a „**občanský zákoník**“), nebo se jedná o jiné informace, které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS:

Obchodní tajemství či jiné informace dle § 3 odst. 1 ZRS	Umístění ve smlouvě či jejích přílohách
Zvolte položku.	Klikněte sem a zadejte text, např. „ Čl. 6 odst. 6.1 smlouvy .“
	Klikněte sem a zadejte text.
	Klikněte sem a zadejte text.

Účastník tímto čestně prohlašuje, že údaje a skutečnosti uvedené ve smlouvě, která je nedílnou součástí nabídky, označené jako obchodní tajemství, naplňují současně všechny definiční znaky obchodního tajemství, tak jak je vymezeno v ustanovení § 504 občanského zákoníku, tj. obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastníky zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení. Účastník dále čestně prohlašuje, že nese veškerou odpovědnost v případě, že část obsahu smlouvy, která se týká obchodního tajemství účastníka a která v důsledku toho bude pro účely uveřejnění smlouvy v registru smluv znečitelněna, pokud by smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, zda byla smlouva uveřejněna prostřednictvím registru smluv ze strany zadavatele nebo účastníka.

Účastník tímto čestně prohlašuje, že neprodleně písemně sdělí zadavateli skutečnost, že takto označené informace přestaly naplňovat znaky obchodního tajemství.

Účastník tímto čestně prohlašuje, že údaje a skutečnosti uvedené ve smlouvě, která je nedílnou součástí nabídky, jsou údaji nebo skutečnostmi (s výjimkou obchodního tajemství, uvedeného výše), které nemohou být v registru smluv uveřejněny na základě ustanovení § 3 odst. 1 ZRS. Účastník dále čestně prohlašuje, že nese veškerou odpovědnost v případě, že část obsahu smlouvy, která obsahuje informace označené účastníkem jako informace ve smyslu § 3 odst. 1 ZRS a která v důsledku toho bude pro účely uveřejnění smlouvy v registru smluv znečitelněna, pokud by smlouva v důsledku takového označení byla uveřejněna způsobem odporujícím ZRS, a to bez ohledu na to, zda byla smlouva uveřejněna prostřednictvím registru smluv ze strany zadavatele nebo účastníka.

V dne

Příloha č. 13 zadávací dokumentace

Čestné prohlášení účastníka ke střetu zájmů

Účastník:

Obchodní firma/jméno
Sídlo/místo podnikání
IČO
Zastoupen

který podává nabídku v řízení na zadání nadlimitní sektorové veřejné zakázky s názvem „**Log management a SIEM**“, č.j. **61441/2023-SŽ-GŘ-08** (dále jen „**Veřejná zakázka**“ a „**Zadávací řízení**“), tímto čestně prohlašuje, že:

- a. **není** obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „**Zákon o střetu zájmů**“), nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti, a
- b. žádní poddodavatelé, jimiž prokazuje kvalifikaci v Zadávacím řízení, **nejsou** obchodní společností, ve které veřejný funkcionář uvedený v ust. § 2 odst. 1 písm. c) Zákona o střetu zájmů nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti.

Účastník dále čestně prohlašuje, že dostane-li se Účastník nebo poddodavatel, jímž prokazoval kvalifikaci v Zadávacím řízení, do střetu zájmů dle § 4b Zákona o střetu zájmů, a to kdykoliv až do okamžiku ukončení Zadávacího řízení, oznámí tuto skutečnost bez zbytečného odkladu zadavateli Veřejné zakázky.

Účastník si je vědom všech právních důsledků, které pro něj mohou vyplývat z nepravdivosti zde uvedených údajů a skutečností.

V dne

Příloha č. 14 zadávací dokumentace

Čestné prohlášení účastníka o splnění podmínek v souvislosti se situací na Ukrajině

Účastník řízení:

Obchodní firma/jméno

.....

Sídlo/místo podnikání

.....

IČO

.....

Zastoupen

.....

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Log management a SIEM**“, č.j. **61441/2023-SŽ-GŘ-08** (dále jen „**Veřejná zakázka**“ a „**Zadávací řízení**“), tímto čestně prohlašuje, že:

- a. on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v Zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, **nejsou** osobami dle článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění pozdějších předpisů,
- b. on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v Zadávacím řízení, ani žádný z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání veřejných zakázek, **nejsou** osobami dle článku 2¹ nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů, a dalších prováděcích předpisů k tomuto nařízení Rady (EU) č. 269/2014 (**tzv. sankční seznamy**)².

Účastník dále čestně prohlašuje, že přestane-li on sám jakožto dodavatel, případně dodavatelé v jeho rámci sdružení za účelem účasti v Zadávacím řízení, nebo některý z jeho poddodavatelů nebo jiných osob, jejichž způsobilost je využívána ve smyslu evropských směrnic o zadávání

¹ Dle článku 2 nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění pozdějších předpisů, nesmějí být žádné finanční prostředky ani hospodářské zdroje přímo ani nepřímo zpřístupněny fyzickým nebo právnickým osobám, subjektům či orgánům nebo fyzickým nebo právnickým osobám, subjektům či orgánům s nimi spojeným uvedeným v příloze I Nařízení nebo v jejich prospěch.

² Zejm. Prováděcí nařízení Rady (EU) 2022/581 ze dne 8. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny a prováděcí nařízení Rady (EU) 2022/658 ze dne 21. dubna 2022, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny a prováděcí nařízení Rady (EU) 2023/429 ze dne 25. února 2023, kterým se provádí nařízení (EU) č. 269/2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny.

veřejných zakázek, splňovat výše uvedené podmínky, k nimž se toto čestné prohlášení vztahuje, a to kdykoliv až do okamžiku ukončení Zadávacího řízení, oznámí tuto skutečnost bez zbytečného odkladu, nejpozději však **do 3 pracovních dnů** ode dne, kdy přestal splňovat výše uvedené podmínky, k nimž se toto čestné prohlášení vztahuje, zadavateli Veřejné zakázky.

Účastník si je vědom všech právních důsledků, které pro něj mohou vyplývat z nepravdivosti zde uvedených údajů a skutečností.

V dne

Příloha č. 15 zadávací dokumentace

Seznam poddodavatelů

Účastník:

Obchodní firma/jméno
Sídlo/místo podnikání
IČO
Zastoupen

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Log management a SIEM**“, č.j. **61441/2023-SŽ-GR-08**, tímto předkládá v souladu s § 105 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, seznam poddodavatelů, s jejichž pomocí předpokládá plnění veřejné zakázky.

Identifikace poddodavatelů dodavatele ¹			Část plnění veřejné zakázky, které má dodavatel v úmyslu zadat poddodavateli (specifikace a procentuální podíl)
1.	Obchodní firma / jméno a příjmení	[doplň dodavatel]	[doplň dodavatel]
	Sídlo / Místo podnikání	[doplň dodavatel]	
	Identifikační číslo	[doplň dodavatel]	
	Prostřednictvím poddodavatele prokazována kvalifikace	ANO/NE [doplň dodavatel]	

V dne

¹ V případě více poddodavatelů zkopíruje dodavatel tabulku tolikrát, kolikrát bude třeba.

Příloha č. 16 zadávací dokumentace

Čestné prohlášení ke splnění základní způsobilosti

Účastník:

Obchodní firma/jméno

.....

Sídlo/místo podnikání

.....

IČO

.....

Zastoupen

.....

který podává nabídku na nadlimitní sektorovou veřejnou zakázku s názvem „**Log management a SIEM**“, č.j. **61441/2023-SŽ-GR-08**, tímto pro účely prokázání základní způsobilosti dle § 74 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), čestně prohlašuje, že je dodavatelem

- 1) který nemá v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek ve vztahu ke spotřební dani;
- 2) který nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění;
- 3¹⁾ který není v likvidaci², proti němuž nebylo vydáno rozhodnutí o úpadku³, vůči němuž nebyla nařízena nucená správa podle jiného právního předpisu⁴ nebo v obdobné situaci podle právního řádu země sídla dodavatele.

V dne

¹ Čestné prohlášení ve vztahu k § 74 odst. 1 písm. e) ZZVZ předkládá dodavatel v případě, že není zapsán v obchodním rejstříku.

² § 187 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

³ § 136 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.

⁴ Například zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, zákon č. 87/1995 Sb., o spořitelních a úvěrních družstvech a některých opatřeních s tím souvisejících a o doplnění zákona České národní rady č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů, zákon č. 363/1999 Sb., o pojišťovnictví a o změně některých souvisejících zákonů.

PTK I	PTK II
Caleum a.s.	O2 Czech Republic a.s
Next Generation Security Solutions s.r.o.	IXPERTA s.r.o.
COMGUARD a.s.	ALEF NULA, a.s.
AMI Praha a.s.	Rexonix security s.r.o
AXENTA a.s.	COMGUARD a.s.
O2 Czech Republic a.s.	ISECO.CZ s.r.o.
NEWPS.CZ s.r.o.	NEWPS.CZ s.r.o.
ALEF NULA, a.s.	
REXONIX SECURITY s.r.o.	

Pozn.: Některé odpovědi účastníků PTK I a II byly pro účely zadávacího řízení anonymizovány. Pro nahrazení byly použity XXXXXX, nebo YYYYYY.

Kategorie	Dotaz v rámci PTK I	Účastník 1	Účastník 2	Účastník 3	Účastník 4	Účastník 5	Účastník 6	Účastník 7	Účastník 8	Účastník 9
Centrální vs. decentralizovaný sběr logů	Uveďte, které z uvedených variant přístupu k řešení sběru logů podporuje vaše řešení.	Není uvedeno jednoznačně, ale z architektury řešení lze usuzovat, že řešení podporuje obě varianty.	CLOUD řešení	Obě varianty	Nabízené řešení podporuje obě varianty sběru auditních dat (logů).	Obě varianty	Obě varianty	CLOUD řešení	O2 SEC podporuje varinatu centrálního a decentralizovaného uložště logů.	Obě varianty
Centrální vs. decentralizovaný sběr logů	Uveďte klíčová kritéria pro rozhodnutí, která varianta je vhodná v jakých situacích.	Neuvedeno	CLOUD řešení	Klíčovým faktorem je topologie sítě z hlediska bezpečnosti a nastavení. Mohou všechny sledované cíle přistupovat do centrálního úložiště nebo je komunikace povolena jen v rámci dané subsítě a odeslání logů do centrálního bodu je možné pouze z jednoho definovaného serveru? Dalším kritériem je disková kapacita na místě uložení sebraných logů a možnosti jejího zabezpečení a zajištění.	Klíčovými kritérii při rozhodování mezi centralizovaným a decentralizovaným sběrem auditních dat jsou faktory jako rozložení zátěže, síťové nebo geograficky oddělené lokality, organizační dělení (tenanti), lokality s omezenou konektivitou.	1. Síťová topologie. 2. Šířka pásma mezi jednotlivými lokalitami. 3. Dostupnost Datacenter a dostupnost strojových zdrojů (CPU, RAM, HDD)	Doporučený postup formou pilotních projektů, postupného nasazení a průběžného školení řešení dle reálných potřeb zákazníka. Nasazení decentralizované varianty nicméně nevylučuje nasazení s centralizovaným řešením	CLOUD řešení	Neuvedeno	1. Existují odločené lokality, které vyžadují lokální sběr? (kapacita linek, jiné omezení) 2. Máme garanci, že nemůže po cestě dojít k odstranění nebo modifikaci auditního logu? 3. Chceme mít některé typy logů dostupné pro analýzu v řádu jednotek sekund, nebo nám stačí dávkový sběr např. 1x za hodinu? 4. Už existuje vlastní sběr pro některé typy logů? (např. WEC pro sběr logů z windows serverů, syslog pro unix servery)
Centrální vs. decentralizovaný sběr logů	Popište vrcholovou architekturu pro všechny vámi doporučené varianty řešení.	Uvedena celková architektura řešení	CLOUD řešení	Uvedena celková architektura řešení	Pro centralizovaný sběr logů je možnou architekturou nasazení formou „All-In-One“ appliance (volitelně v HA), s možností přidání jednotlivých kolektorů v případě potřeby. Decentralizovaný sběr událostí lze nasadit pomocí centrálního řídícího prvku, samostatných boxů pro uložení a zpracování událostí (například v jednotlivých lokalitách) volitelně doplněných o potřebný počet kolektorů.	Uvedena celková architektura řešení	Uvedena celková architektura řešení	CLOUD řešení	Uvedena celková architektura řešení	Neuvedeno
Transport logů od zdrojů logů (Log Sources) do Log Managementu	Uveďte, zda a jak vaše řešení přímo podporuje zajištění kompletního přenosu logů od zdroje až k místu pro vyhodnocování logů.	Ano, naše zařízení sbírá logy přímo anebo nepřímo z daných datových zdrojů	CLOUD řešení	Logy jsou načítány kontinuálně tak, jak vznikají. K zajištění kvality/úplnosti přenosu slouží standardní nástroje poskytované protokolem TCP. K zabezpečení transportu se může použít protokol https + ověřovací tokeny jednotlivých komponent.	Pro Microsoft Windows OS je pro řešení dostupný agent, který zajišťuje sběr a zasílání událostí do řešení, nicméně není nutnost tohoto agenta využívat. Pro ostatní zdrojové systémy řešení podporuje univerzální typy sběru logů jako je Syslog, TLS Syslog, JAB, nebo u cloudových řešení API jednotlivých výrobců. Řešení pak následně zajišťuje případný přenos logů z místních kolektorů do místa zpracování pomocí šifrovaného SSH tunelu.	1. Sbíráni pomocí agenta (Splunk Universal Forwarder) 2. Posílání dat na sdírné místo (Splunk Heavy Forwarder) 3. Dotazování se na data – do databáze, API, ... (Splunk Heavy Forwarder)	Ano, řešení podporuje kompletní přenos logů od zdroje.	CLOUD řešení	Na straně Objednatele jsou sbírány logy z definovaných zařízení. Ty proudí do tzv. kolektorů. To jsou sběrná místa v síti Objednatele instalované jako virtuální zařízení v HA nastavení v DMZ a NonHA v LAN siti Objednatele. Tyto kolektory slouží ke sběru logů z jednotlivých zdrojů Objednatele. Krátkodobý výkon jednoho kolektoru přesahuje 10000 EPS.	Součástí nabízeného řešení jsou automaticky sw komponenty pro zajištění samotného sběru. Tyto komponenty se samostatně nelicencují a jsou automaticky součástí licence v neomezeném množství sběrných konektorů, lokalit apod.
Transport logů od zdrojů logů (Log Sources) do Log Managementu	Uveďte doporučení, zda je vhodné, aby si Zadavatel realizoval transportní vrstvu interními silami. Jaké jsou výhody a nevady takového přístupu?	Mezistupeň nedoporučujeme	CLOUD řešení	Zákazník si může zajistit distribuaci logů do úložiště, ze kterých budou naše systémy číst data ke zpracování a tím eliminovat nutnost přístupu ze sledovaných zařízení na servery s našimi řešeními. To by bylo výhodné například tehdy, pokud by nebyl dopředu známý počet sledovaných zařízení. Nevýhodou takového řešení je přírůstkové čtení dat z tohoto úložiště místo přímého propojení sledovaných systémů na síťové úrovni.	Ano, omezení vendor lock-inu.	Uchazeč doporučuje, aby sběr logů zajistil stejný tým, který dodává a spravuje Log Management.	Transportní vrstva by měla být realizovaná dohromady s dodavatelem či výrobcem systému Logmanager.	CLOUD řešení	Realizace transportní vrstvy mezi zdrojem logů a kolektorem (Advanced collector) je vždy v kompetenci Zadavatele. O2 SEC jako Dodavatel je v rámci implementace řešení připraven poskytnout plnou součinnost.	Využití vlastní transportní vrstvy dává smysl pouze v případě, že už jí zadavatel disponuje a splňuje všechny jeho parametry z pohledu dostupnosti, integrity a důvěrnosti. Pokud by jí teprve implementoval, nezíská tím asi žádnou výraznou přidanou hodnotu.
Transport logů od zdrojů logů (Log Sources) do Log Managementu	Jaké jsou možnosti využití vašeho řešení v případě, že se Zadavatel snaží vyhnout vendor lock-inu prostřednictvím oddělení transportní vrstvy?	Neuvedeno	CLOUD řešení	Pokud se zákazník snaží vyhnout vendor lockinu z hlediska sebraných dat, umí naše systémy přeposílat data v původní podobě do záložního systému zadavatele nebo lze zlohotovat/archivovat sbírané logy na úrovni jejich zdrojů. Navíc i v případě ztráty licence a tedy nemožnosti data dále sbírat, zachovává systém již sebraná data přístupná administrátorovi	Řešení umožňuje samostatný sběr událostí či možnost přeposílání událostí z vlastní transportní vrstvy. Doručení RAW logu z transportní vrstvy umožňuje práci LM i SIEM stejně jako by události byly sbírány přímo.	Uchazeč podporuje více způsobů sběru logů, nevyžaduje tedy zvláštní úpravy prostředí, které by vedl k vendor-lockinu.	Logmanager využívá pro sběr logů primárně standardizované protokoly Syslog (UDP/TCP/TLS) a RELP. Sběr agenty nebo komponenty Logmanageru je použit pouze v případě, že formát nebo dostupnost logů neumožňuje využití standardizovaných protokolů. Logmanager Beat Agent není licenčně omezen a lze jej nahradit opensource Elastic Search WinLogBeat a FileBeat, nicméně tyto již neposkytují možnost centralizované konfigurace ani automatické aktualizace.	CLOUD řešení	Řešení je koncipováno jako otevřené, to znamená, že použité technologie jsou Open-Source, což znamená rozsáhlou komunitu a snadné dohledávání technických a provozních informací. Dále je řešení dodáváno spolu se všemi zdrojovými kódy, takže jej můžete snadno rozšiřovat a nehrázit tzv. vendor-lock.	Neuvedeno

Vztah řešení Log Management a SIEM (Security Information and Event Management)	Pokud zadavatel plánuje budoucí nasazení řešení SIEM, je vhodné spojit takovou aktivitu s realizací řešení Log managementu? Jaké jsou výhody doporučeného přístupu?	Log Management považujeme jako nedílitelnou část řešení SIEM. Rozdělení nedoporučujeme, jelikož může způsobit výrazně více pracnosti (zejména znovu oddělení dat na jednotlivé datové zdroje a více implementačních prací).	CLOUD řešení	Jednoznačně ano	Ano, výhody spojeného postupu řešení je možnost implementace jednoho řešení místo dvou, zajištění kompatibility LogManagementu a SIEM, úspora nákladů.	ANO spojit LM a SIEM na úrovni technologické platformy, ale držet oddělené projekty, neboť ty na sebe vážou a mají vlastní závislosti (SIEM potřebuje AR, správu aktiv, ...).	Logmanager umožňuje provádění základních SIEM operací ve svém základu. Jediným limitem je časová osa, kdy korelace prováděné v reálném jsou limitované pro maximálně 30minutové okno. Nicméně Logmanager umožňuje vytváření velmi snadných pravidel pro export vybraných událostí na externí systémy nejsnadněji na základě značek (tagů) na externí systémy.	CLOUD řešení	Z provozního a ekonomického hlediska je dle zkušeností Dodavatele vhodnější spojit aktivitu nasazení LogManagementu a SIEM do jednoho projektu se společnou architekturou a definováním cílových funkcionalit.	V takto rozsáhlém projektu doporučujeme určitě nasadit nejříve log management a vyřešit všechny související kroky se samotným nastavením auditu jednotlivých technologií, kvalitou auditní stopy, apod. a začít sbírat všechny relevantní informace
Vztah řešení Log Management a SIEM (Security Information and Event Management)	V případě, že vaše řešení poskytuje také funkcionality SIEM, popište je (příp. je poskytněte formou přílohy keší odpovědi v českém nebo anglickém jazyce).	Neuvedeno	CLOUD řešení	Obě naše řešení již obsahují nástroje pro korelace, statistiky, generování událostí, výstrah a grafických prezentací. Systémy obsahují předpřipravené parsery pro různé typy datových zdrojů. Není nijak zvlášť popsáno řešení SIEM.	nabízené řešení podporuje implementaci v režimu LogManagementu s následnou možností rozšíření na SIEM pouze pomocí licence. Krátký přehled funkcionalit je uveden na stránkách výrobce (v anglickém jazyce): https://www.ibm.com/products/gradar-siem	Dodáno jako příloha	jak je napsáno výše, Logmanager podporuje základní SIEM funkcionalitu v základě, bez nutnosti dokupovat speciální licenci.	CLOUD řešení	Neuvedeno	Neuvedeno
Vztah řešení Log Management a SIEM (Security Information and Event Management)	Jaké podmínky pro hladké nasazení SIEM by měl podle vás Zadavatel zajistit v případě odděleného nasazení LM a SIEM?	Oddělovat SIEM a Log Management nedoporučujeme. Doporučuje zvolit etapový přístup – SIEM nejdříve implementovat pro sběr dat ze zdrojů dat a pak dále pokračovat s funkcionalitami SIEM	CLOUD řešení	Dodržet naše doporučení na výkonnost a kapacity infrastruktury, obě řešení umožňují oddělit zpracování sebraných dat z hlediska buď jen sběru logů nebo analýz nad daty obsaženým v sebraných lozích. Práci to znamená společná data, ale odlišné způsoby práce s nimi. Správcům sběru dat není umožněno využívat SIEM vlastnosti a naopak.	Možnosti integrace LM na SIEM, tedy způsob přeposílání událostí, zasílání logů ve stejném formátu jako zdroj (RAW forma), identifikace zdrojových systémů (SIEM musí identifikovat zdrojový systém, ne LM jako zdroj), procesní zajištění přeposílání (jake logy budou z LM zasílány do SIEM).	1. Integrace s LM (přeposílání specifických zpráv do SIEM) 2. Samostatný sběr dat (oddělený od LM) 3. Parsování dat.	Protože v tuto chvíli neznáme zvolené SIEM/SOC řešení, je předběžně definovat podmínky. Obecně se jedná pouze o zadání úkolu pro vývojový team Logmanageru a plnou součinnost při testování.	CLOUD řešení	Při návrhu implementace a jejich fází je třeba počítat s tím, že systémy LM a SIEMu musí být spolu „odladěné“, musí efektivně komunikovat, a to jak v režimu realtime, tak i non-realtime. Současné je velkou výhodou jejich souběžný rozvoj s garancí vzájemné integrity poskytovaných funkcionalit. Tyto vlastnosti přímo ovlivňují schopnost a kvalitu vyšetřování bezpečnostních událostí, a především její časovou náročnost, která patří ke klíčovým parametrům. Společná implementace tak bude mít i přímý pozitivní dopad na zajištění provozu celé platformy, a to i z pohledu adresace odpovědnosti a kompetencí subjektů realizujících implementaci a následný provoz.	začít řešit, jaké Zadavatel podává bezpečnostní scénáře (use cases)
Použití Log Management řešení pro více kontextů, např. zvlášť pro IT (Information Technology) a OT (Operational Technology)	Uveďte klíčová kritéria pro rozhodnutí, v jakých situacích je vhodné oddělit Log Management pro IT/OT a jaké z toho mohou plynout důsledky pro architekturu řešení.	Oddělení nedoporučujeme	CLOUD řešení	Klíčová kritéria vyplývají ze způsobu práce a může se je zákazník definovat. Data můžeme oddělit podle jejich původu. Jsme schopni data fyzicky oddělit a podle potřeby s nimi i tak pracovat jako s celkem, případně umístit data ve společné skupině indexů a podle jejich původu formou oddělených aplikací v rámci řešení nebo na úrovni přístupových práv poskytovat jen relevantní údaje příslušné skupině uživatelů.	Klíčovými kritérii pro rozhodnutí o rozdělení LM pro IT a OT je omezení dostupnosti mezi jednotlivými sítěmi, a tedy možnosti nasazení centrálního řešení.	Uchazeč doporučuje použití jednotného řešení pro IT i OT. Pokud by se však mělo jednat o rozdělení kontextů, tak lze rozdělit prezentační i databázovou vrstvu = tedy přejít k distribuovanému řešení.	Zde neexistuje žádné výrazné omezení. Logmanager umožňuje přidělit libovolné zprávě více značek (tagů) současně, volba přiřazených značek může určit další životní cyklus libovolné zprávy včetně aplikace RBAC, proto libovolná zpráva může být dostupná jak pro oba kontexty, tak pouze pro vybraný kontext	CLOUD řešení	není nutné oddělovat IT a OT, případně je možné řešit v rámci multitenance	Z našeho pohledu není žádný důvod rozdělovat sběr z IT nebo OT do samostatných prostředí.
Použití Log Management řešení pro více kontextů, např. zvlášť pro IT (Information Technology) a OT (Operational Technology)	Popište vrcholovou architekturu pro obě varianty.	Uvedena celková architektura řešení	CLOUD řešení	Uvedena celková architektura řešení	Řešení umožňuje nasazení centralizovaného řešení pomocí tzv. „odpojených kolektorů“, které nevyžadují řídicí příkazy a pouze zasílají data z datové omezených sítí (OT) pouze jedním směrem	Uvedena celková architektura řešení	Vrcholnou architekturu není třeba pro použití s více kontexty speciálně řešit. Logmanager obsahuje komplexní systém řešení RBAC postavený na přístupu k datům prostřednictvím definovaných značek, lze snadno na jedné platformě na základě ověření uživatele snadno řídit přístup k pořízeným datům.	CLOUD řešení	Uvedena celková architektura řešení	Neuvedeno
Provoz řešení v režimu Multi-Tenant	Uveďte, zda vaše řešení podporuje fungování v režimu Multi-Tenant, tedy podporou bezpečné identifikace zdrojových logů různých subjektů, jejich bezpečný přenos, izolované uložení a výslednou interpretaci řízenou dle patřičných přístupových oprávnění.	Multi-Tenant podporujeme na úrovni rolí v systému. Každá role může mít přístup jen k nějakým datům, datovým zdrojům, výstupům a podobně. Data jsou uložena v jednom indexu.	CLOUD řešení	Ano, podporujeme různými způsoby. Podporujeme nad společnými daty různé aplikace, oddělení pomocí přístupových práv i s kombinací oddělení fyzického uložení. Přenos zajišťujeme pomocí https a identifikační tokenů.	Ano, plně konfigurovatelně.	ANO, řešení podporuje Multi-Tenant	Logmanager umožňuje snadné značkování (tagování) logů na základě všech atributů (poil) nacházejících se v libovolné zprávě. Proto následné rozlišení je pouze záležitostí vhodné volby způsobu tohoto značkování.	CLOUD řešení	LM je multitenantní (multitenancy) produkt. To znamená, že umožňuje zpracovávat logy různých subjektů (tzv. tenantů) v oddělených logických prostředích, které ale sdílejí jedno fyzické prostředí (včetně softwarových prostředků a licencí).	Nabízené řešení podporuje Multitenant nasazení, kdy lze řídit pomocí přístupového oprávnění, kdo uvidí jaké logy, tak ho lze zhlídat na straně sběru.

Popište, zda uvažované řešení umožňuje fungování vprostředích, která mají kolizní některé atributy logických aktiv.	Kolize může nastat, systém disponuje funkcí TrueID, kde sjednocuje jednotlivé informace o daném uživateli (IP adresa, doménové jméno, email, login ...) a snaží se pracovat s těmito meta identitami.	CLOUD řešení	ANO, každý záznam se identifikuje typem a názvem datového zdroje a původem (hostname), lze doplnit další kritéria.	ANO	ANO, je více způsobů kterými lze řešit kolizní atributy.	Logmanager umožňuje využití centralizovaného sběru logů prostřednictvím Logmanager Forwarderu (malé fyzické nebo virtuální appliance). Tato appliance sbírá v prostředí s kolidujícími atributy logy stejně jako Logmanager, prostřednictvím protokolu WireGuard předává na centrální datový sklad, nicméně ke všem událostem automaticky přiděluje identifikační značky (tagy) dle volby administrátora.	CLOUD řešení	ANO	Pro spolehlivou identifikaci a nastavení oprávnění je nutné při sběru logů další identifikace a rozdělení logů při sběru, aby bylo patrné z jaké lokality nebo prostředí logy pocházejí. Toto je zvlášť nutné v případě, kdy dochází ke kolizi IP rozsahů apod. Pro samotnou práci s reporty dashboardy apod. je pak nutné používat další parametry, které umožní identifikaci, odkud log pochází. Všechny tyto informace jsou k dispozici při správné implementaci sběru logů.	
	Většina výrobců průměr EPS (MPS) pro své licenční potřeby počítá hodinově. Logrhythm vypočítává tento údaj jako denní průměr (tedy 24h), díky čemuž bývá tato hodnota zpravidla nižší, než u jiných konvenčních výrobců SIEM.	licencována dle počtu tzv. assetů, tedy zařízení s IP adresou v infrastruktuře organizace	Jedno řešení odvozuje licenci od množství zpracovaných dat za jeden den, bez ohledu na rozsah použité funkcionality. Druhé od počtu záznamů zpracovaných za sekundu. Rozsah použitých funkcionalit se také nebere v úvahu.	1. Základní instalační licence 2. Počet nodů řešení 3. V případě nasazení HA počet HA boxů 4. Centrální licence LM (LM neřeší licenční počet nebo velikost události) 5. V případě kombinace se SIEM jsou to EPS a FPM (síťové toky za minutu)	LM: Denní objem uložených dat SIEM: také GB/den, ale pozor, velikost licence SIEM musí být dle doporučení výrobce stejná jako pro základní systém Splunk Enterprise (tedy pro Logmanagement).	Licenční model je velmi intuitivní – jedná se pouze vytvoření clusteru dodatečného počtu Logmanagerů, tak aby zvládali zpracovávat potřebné EPS a také měl dostatečnou kapacitu pro uchování logů. Logmanager jako fyzická appliance nemá licenční omezení na počet zdrojů ani EPS, pracuje do maximálního výkonu použitého hardware modelu. V případě centrálního nasazení a poboček je nutné na každou pobočku nasadit buď Logmanager Forwarder, který zajišťuje zabezpečený přenos dat i konfiguraci přes nedůvěryhodné prostředí. Logmanager Forwarder, v případě, že se jedná o jeho virtuální verzi, je samostatně licencován pouze na množství instalovaných instancí.	Licencován je počet stanic a velikost prostoru v cloudu zaplněný logy z infrastruktury formou cloud licence subscription. Je možné zakoupit jednotlivé moduly na omezené časové období.	O2 SEC dohled je dodáván formou služby – licenční podmínky jsou řešeny na straně Dodavatele služby.	Nabízené řešení se licencuje pouze podle jednoho parametru a to počtu událostí za sekundu v průměru (EPS). Tato hodnota se stanoví tak, že se každých 24 hodin sečte počet uložených logů a vydělí časem, získáme průměrnou hodnotu EPS za daný den.	
	ANO	nedostatečné	nedostatečné	ANO	ANO	ANO	ANO	ANO	ANO	Neuvedeno V rámci už vypsáno a později zrušeného VŘ Zadavatel uvedl dostatek informací pro sestavení nabídky a její odevzdání.

		Účastník 1	Účastník 2	Účastník 3	Účastník 4	Účastník 5	Účastník 6	Účastník 7
Odpověď	Indikace nákladů (celkem na 5 let) - varianta 1	66 857 500 Kč	56 997 120 Kč	34 856 000 Kč	68 120 200 Kč	27 044 365 Kč	60 894 802 Kč	50 306 683 Kč
Odpověď	Indikace nákladů (celkem na 5 let) - varianta 2	93 880 000 Kč	96 099 216 Kč	59 356 000 Kč	128 722 100 Kč	38 856 100 Kč	90 267 780 Kč	103 580 007 Kč
Odpověď	Celkem vCPU - varianta 1	680	288	472	432	N/A		
Odpověď	Celkem RAM - varianta 1	744	2048	544	512	N/A		
Odpověď	Celkem storage - varianta 1	329600	136000	45732	44608	N/A		
Odpověď	Celkem backup storage - varianta 1	320760				N/A		
Odpověď	Celkem vCPU - varianta 2	872	544	864	784	N/A	504	384
Odpověď	Celkem RAM - varianta 2	904	4864	1536	1408	N/A	4032	1376
Odpověď	Celkem storage - varianta 2	616400	556000	85632	84608	N/A	1543344	62900
Odpověď	Celkem backup storage - varianta 2	607060	N/A	N/A	N/A	N/A	3700	172
Dotaz na účastníka	Účastník uveďte pouze jednu specifikaci požadavků na výpočetní výkon Zadávatel. Je tento výkon požadovaný pro variantu 1 nebo variantu 2?	x						x
Dotaz na účastníka	Vámi indikovaná požadovaná disková kapacita se při našich znalostech zdá být o řád vyšší. Můžete prosím potvrdit, že byla uvedena správná hodnota pro jeden virtuální systém. Při hodnocení vyplněných informací provádíme násobení všech uvedených hodnot, vCPU, RAM a diskové kapacity, uvedeným počtem kusů virtuálních systémů.	x					x	

Kategorie	Dotaz v rámci PTK II	Splnění požadavku (Ano/Ne/Částečně)	Splnění požadavku (Ano/Ne/Částečně)	Splnění požadavku (Ano/Ne/Částečně)	Splnění požadavku (Ano/Ne/Částečně)	Splnění požadavku (Ano/Ne/Částečně)	Splnění požadavku (Ano/Ne/Částečně)	Splnění požadavku (Ano/Ne/Částečně)
Architektura	Zadávatel umožňuje využití dvojice datových center, k umístění a provozu centrálních komponent řešení Log management a SIEM. Navrhněte vhodný způsob využití těchto DC, např: - budeme využívat jen pro účely archivace - nebo bude realizovaný plnohodnotný cluster - jiný způsob využití	Splunk plně podporuje redundanci. Index i Search vrstva podporuje i clusterové řešení. Jen musíme upozornit, že provozování Cluster řešení jen v rámci dvou DC není optimální, a při výpadku jednoho celého DC bude nutný ruční zásah. Cluster vyžaduje minimálně 3 členy.	Dvě datové centra se mohou využít pro disaster recovery v případě výpadku jedné lokality. Funkce SIEMu by byla rozprostřena přes dvě lokality. Tedy využití primárně pro DR cluster pro případ výpadku funkce řízení a zpracování eventů na jedné lokalitě se předá řízení na druhou lokalitu.	Instalace SIEM řešení v distribuované variantě jako virtual appliance a zároveň ve vysoké dostupnosti (využití obou datových center v případě splnění parametrů na propustnost linky a latence). 2x SIEM Konzole v HA zapojení, 2x SIEM Event Processor v HA zapojení, 2x SIEM Event Collector v HA zapojení (jeden node v každém DC) a 16x Event Collector v remote geo lokalitách (variantně i tyto kolektory v HA).	Instalace SIEM řešení v distribuované variantě jako virtual appliance a zároveň ve vysoké dostupnosti (využití obou datových center). 2x SIEM Konzole v HA zapojení, 2x SIEM Event Processor v HA zapojení a 16x Event Collector v remote geo lokalitách.	Systém může běžet v pacemaker cluster systému v aktiv pasiv konfiguraci. Případě lze zajistit běh dvou nezávislých SIEM nódů, kde se data z prvního nódu po normalizaci a parsování forwardují na druhý nód. Zálohu raw dat lze řešit replikou na úrovni pole nebo rsyncem archivních dat do druhé lokality.	Nasazení centrálních komponent řešení Log management a SIEM bude provedeno do obou datových center zadavatele v režimu active/active, tj. jako geografický cluster, který poskytuje redundanci vysokou dostupnost. Optimální by byla ještě jedna malá lokalita (může být třeba Microsoft Azure), kde je provozován malý VM, který slouží jako arbitr pro případ tzv. "split-brain" problému.	Architektura řešení je variabilní, doporučujeme používat cluster rozprostřený přes obě DC, který umožňují plnou funkcionalitu i při kompletní výpadku jedné strany. Případně lze upravit i požadavky zákazníka během analýzy. HLD je součástí samostatné přílohy. Všechny komponenty řešení je možné provozovat ve virtuálním prostředí a proto navrhujeme vše postavit na virtualizační platformě zákazníka (viz samostatný excel)
Architektura	Jaké budou účely a parametry využití propoje mezi dvojicí DC v Praze: - jaké jsou v navrhované variantě požadované parametry propoje dvou DC - jak bude ve vybrané variantě vypadat využívání propoje dvou DC: - forwardování událostí z jedné lokality do druhé - replikace na úrovni DB - vícenodové zpracování a parita dat	Index vrstva využívá interní databázi typu NoSQL (nejedná se ale o žádná standardizovaná řešení). Systém si sám zajišťuje replikaci dat mezi členy clusteru. Latence mezi členy clusteru (včetně různých DC) musí být menší než 100ms. Požadavek na rychlost linky přímo není definován, ale rychlost musí být dostatečná s ohledem na objem příchozích dat a tedy i s ohledem na požadovanou replikaci.	Účel propoje bude replikace DB mezi lokalitami. Propoj mezi lokalitami musí být stabilní linka s nízkou latencí - půjde v převážné míře o replikace dat mezi lokalitami.	Pro nejlepší výkon ve vysoké dostupnosti se důrazně doporučuje použít rozhraní 10 Gb/s. Použití rozhraní 10 Gbps zkracuje čas potřebný pro synchronizaci systému a zajišťuje optimální výkon. Latence na lince mezi DC by neměla překračovat průměr 2 milisekundy.	Pro nejlepší výkon ve vysoké dostupnosti se důrazně doporučuje použít rozhraní 10 Gb/s. Použití rozhraní 10 Gbps zkracuje čas potřebný pro synchronizaci systému a zajišťuje optimální výkon.	Robustnost replikace dat lze šklovať. Forward událostí, replikace, lze i provést forward událostí z SIEM do DB a následně provést replikaci na úrovni DB.	Geografický cluster vyžaduje privátní "subnet" na L2 nebo L3 úrovni, který je plnohodnotně přístupný ze serverů (uzlů clusteru) v data centrech. Požadavky na konektivitu jsou cca 1Gbps ve špičce, není třeba vyhrazený spoj. Pro propojení postačuje bezpečně izolovaná VLAN. V navrhovaném režimu jsou data zpracováváná na více uzlech clusteru dle nastaveného replikačního faktoru, zde navrhujeme 2. Databázová vrstva je rovněž replikována.	Propoj mezi DC bude primárně používán pro interní komunikaci komponent LM a SIEMu. Viz architektura, doporučujeme vybudování clusteru rozprostřeného mezi obě DC. Architekturu řešení lze upravit a je možné vybudovat naprosto nezávislý cluster v každém DC. Podrobnosti viz samostatná příloha s popisem architektury.
Funkcionalita	Podporuje řešení logy pouze zasílat do Log managementu, aby nebyly vyhodnocovány v SIEMu, bez čerpání licence SIEMu.	Vytvoří se oddělený Index Cluster, tím se zajistí potřebná funkcionalita. V tomto případě LogManagement má dostupná všechna data bez omezení (z obou Index Clusterů). Licence na LogManagement se tímto nijak neovlivňuje a licence musí pokrývat objem všech dat. SIEM část má ale data dostupná jen z jednoho Index Clusteru. Tím lze šetřit SIEM licenci. Na vstupu se musí definovat pravidlo, pomocí kterého se rozliší, zda data mají jít do SIEM nebo do LogManagement indexu.	Řešení obsahuje Log Management. Složitější funkce SIEMu se nemusí využívat. SIEM je neúplnou součástí řešení a obecně není dobré mít rozdělený tyto součásti samostatně.	Ano, pomocí licenčního rozšíření (součástí nabídky) lze pomocí filtrů označit logy, které neprocházejí korelačním enginem a jsou zpracovány jen v rámci log managementu a nepočítají se vůči licenci.	Specificky na jednotlivém Log Collectoru je možné definovat (nastavit) přeposílání logů tak, aby neprocházejí korelačním enginem, tzv. funkcionalita Forward and Bypass Correlation	Licence je na počet EPS a není rozdílná, zda-li se využije jen log management a celá funkcionalita SIEM, lze provést samostatně nezávislé uložení logů do souborů, ale to úplně bypasse SIEM řešení.	Obě řešení mají vlastní licenci a zákazník si vybírá, co chce v jaké části zpracovávat. Takto lze ušetřit část licence na SIEM a je to námi doporučená varianta.	

Funkcionalita	Podporuje řešení rozdílné retence pro určité typy logů?	Retence dat se aplikuje na tzv. Index. Počet indexů není nijak omezen. Na vstupu je nutno definovat, kam se která data mají posílat (do kterého indexu).	Vybrané logy jsou vyřazeny z dalšího zpracování v rámci indexace DB a retence v archivech. Obecně nedoporučujeme mít rozdílnou retenci, vzhledem k tomu, že mohou pak chybět podstatné doplňující informace při prošetřování incidentů v rámci budoucího zpracování v rámci SOCu. Úspory dat se dá docílit i filtrací logů na podstatné a nepodstatné informace, zvláště u zařízení nezapadající do množiny systémů kritické infrastruktury.	Řešení umožňuje tvorbu tzv. Retention buckets, kde lze pomocí filtrů rozdělit data na jednotlivé části s odlišnou retencí.	Řešení umožňuje tvorbu tzv. Retention Buckets, kde pomocí filtrů nastavíme retenci uchovávaných dat pro specifickou source IP adresu nebo specifický Log source.	Použití logu forwardingu na základě podmínek, export do DB s retencí atd.	Jednotlivé typy logů jsou umístěny do tzv. datasetů. Každý dataset může definovat vlastní retenci pomocí tzv. "životního cyklu".	Lze určovat samostatně retence jak pro typy logů, dle konkrétního zdroje, podle skupin (produkční, testovací prostředí, autentizace, apod.)
Funkcionalita	Podporuje nástroj možnosti live dashboardů pro team SOC, kde je možno zobrazovat trendové grafy např. firewall deny, připojení do VPN za posledních 24h a možnost zobrazovat tyto dashboardy na zobrazovacích plochách s automatickým refreshem?	Každý dashboard může mít nastaven automatický refresh a také u každého dashboardu definujeme po jakém čase má dojít k refresh. Pro specifické případy lze využít i tzv. realtime dotazu, kdy se aktualizace dat provádí online ihned po zpracování dat systémem.		Řešení obsahuje několik předpřipravených reportů, dashboardů a vizualizací, které jsou upravitelné. Zároveň podporuje vlastní tvorbu reportů, dashboardů a jiných výstupů (grafů, tabulek apod.). Lze připravit vlastní výstup na libovolných normalizovaných atributech (properties) od daného okamžiku historie. Řešení obsahuje přívětivého grafického průvodce, který vede k jejich snadnému vytvoření.	Řešení obsahuje několik předpřipravených reportů, dashboardů a vizualizací, které jsou upravitelné a očekává se, že si je zákazník dále upraví. Zároveň podporuje vlastní tvorbu reportů, dashboardů a jiných výstupů (grafů, tabulek apod.). Lze připravit vlastní výstup na libovolných normalizovaných atributech (properties) od daného okamžiku historie. Řešení obsahuje přívětivého grafického průvodce, který vede k jejich snadnému vytvoření.	Dashbordy a grafy v MySentinel, grafy v realtime view, security intelligence Dashboard interní Kibana a Elasticsearch, externí Kibana a Elasticsearch, externí relační databáze na základě filtru exportované data s nasazením zobrazení a agregace dat.	Navrhované řešení poskytuje vlastní dashboard komponentu, které umožňuje zobrazovat trendové grafy, definovat "playlisty" i s automatickým refreshem. Dále je možné využít i nástroje Kibana a Grafana, které jsou s řešením kompatibilní.	Nástroj obsahuje konzole pro použití v režimech SOC s uvedenými parametry
Funkcionalita	Může být log collector virtuální?	Veškeré komponenty jsou dodávány jako standardní SW instalační balíček popřípadě i výrobce dodává image pro kontejnery. Tedy celé řešení lze provozovat virtualizovaně.			Může být jak hardwarový, tak virtuální. S ohledem na jiný životní cyklus software a hardware, je dnes většina instalací virtuálních. V případě instalace je použit shodný instalační soubor, při jehož spuštění se vybírá, jaké komponenty se nainstaluje, včetně Event Processor, Event Collector, Console, AppHost pro rozšiřující nadstavbové aplikace apod. Výrobce ve své dokumentaci jasně uvádí, jaká komponenta s jakou EPS licenci požaduje patřičné zdroje (vRAM, vCPU apod.)		Log kolektor se dodává i formou obrazu virtuálního stroje (VM).	Preferovaná varianta pro redukci nákladů a snazší správu
Funkcionalita	Může mít log collector více síťových interface?	Více síťových interface je plně podporován a v praxi i velmi často využíván. Je podporován na všech komponentech našeho řešení.						Pouze záleží na konfiguraci OS
Funkcionalita	Po jakou dobu či množství dat log collector umožní ukládat logy při nedostupnosti centrálního řešení ?	Kolektory mají vlastnost nazývanou Permanent Cache nebo Persistent Queue. Musí se explicitně zapnout. Data se pak ukládají na disk, aby nedošlo ke ztrátě. Zároveň dojde k propagaci BLOCK stavu na vstupní konektory a jedná se o snahu zablokovat již systém, který generuje data. Po obnovení spojení se data odesílají v pořadí, jak do systému přišla.	Je omezeno místem na disku daného kolektoru. Obecně ale nelze doporučit výpadek déle než 1-2 dny z důvodu zpracování těchto informací v runtime v rámci SOC use-casů.	QRadar Event Collector ukládá data do diskové cache v případě nedostupnosti Event Processoru (který zpracovává data a ukládá je). Velikost diskové cache je omezena pouze velikostí disku připojeného k Event Collectoru.	Nabízené řešení má dvě důležité komponenty, a to je Event Collector a Event Processor. Collector sám o sobě data neukládá, pouze normalizuje a zpracovává eventy a následně je odesílá do Event Processor, kde se vyhodnocují oproti definovaným pravidlům. Eventy se ukládají na straně Event Processor. V krajních případech lze využít funkčnost Store and Forward na Event Collector, kdy se předzpracované eventy odesílají do Event Processor v nastaveném časovém okně, kdy je Collector připojen na síť (využití například v remote lokalitách, zaoceánské lodě, systémy, které se dostávají mimo 4G/5G signál).	Záleží na konfiguraci buferu po 1 hodině časového rozdílu, nebudou se zpracovávat korelace, pokud je zapnuto věřit času ze zdroje.	Toto závisí na dostupném diskovém uložišti kolektoru. Jedná se řádově o dny.	Při výpadku posílání logů mají sběrné konektory cache, ve které se drží logy do opravy výpadku. Tato doba je omezena jen velikostí diskové kapacity. Standardně doporučujeme její dobu 5-7 dní. Tato cache funguje i pro logy zaslané syslogem
Funkcionalita	Jak řešení řeší jednorázové vysoké množství přijímaných logů, které přesahuje licenci?	Objem přijímaných dat se kontroluje jednou za den. Pokud dojde překročení licence, generuje se WARNING stav. U licence větší než 100GB za den nedochází k žádné další reakci. Tedy zákazník se dozví, že překračuje licenci ale jinak systém běží bez jakéhokoli omezení.	Překročení licence je jen informace, že k tomu došlo. Řešení umí zpracovávat peaky eventů. Zpracování informací překračující licenci je omezeno jen výkonem použitého HW.	Před zpracováním příchodného Eventu se kontroluje aktuální využití licence EPS. Pokud je licence překročena, event se zařadí do lokálního buferu a k jeho zpracování dojde v momentě, kdy náhla špička zpracovávaných eventů opadne.	Před zpracováním příchodného Eventu se kontroluje aktuální využití licence EPS. Pokud je licence překročena, event se zařadí do lokálního buferu a k jeho zpracování dojde v momentě, kdy náhla špička zpracovávaných eventů opadne.	Neděje se nic, řešení poskytuje službu, pouze je nutné navýšit počet licencí.	Navrhované řešení neobsahuje žádný "tvrdý" limit, který by omezoval příjem logů dle licence. Řešení logy přijímá i když přesahují licenční limit. Překročení je pak indikováno v telemetrii a řešeno obchodně. Řešení umožňuje i konfiguračně omezit maximální průtok, pak jsou logy zařazeny do fronty a zpracovány se zpožděním.	Řešení je licencováno na bázi denního průměru EPS. Při jeho překročení dojde pouze k indikaci tohoto stavu administrátorovi řešení a nedojde k žádnému omezení funkcionality

Funkcionalita	Popsište, jak se v řešení provádí drilldown analýza.	Každý report v rámci dashboardu má podporu DrillDown. Tedy proklikat se níže při řešení a dostat se ke kořeni věci. DrillDown může být automatický nebo manuální. Při manuálním se mohou definovat vlastní drilldown dotazy. Používá se velmi často jako proklik do jiného dashboardu nebo propojení s dalšími daty.	Dropdown analýza probíhá klikáním ve WebGUI a pomocí DrillDown do podrobnějších náhledů pro danou informaci až úplně na raw log, pokud to analytik požaduje.	Pokud se má na myslí drill-down analýza, tak řešení poskytuje unifikovaný náhled na vzniknutý incident a veškeré eventy/logy, které s ním souvisí. Administrátor, který řeší daný incident tak může přímo z popisu incident zkoumat jednotlivé eventy a prohlédávat pomocí filtrů veškerá sbíraná data.	Pokud se má na myslí drill-down analýza, tak řešení poskytuje unifikovaný náhled na vzniknutý incident a veškeré eventy/logy, které s ním souvisí. Administrátor, který řeší daný incident tak může přímo z popisu incident zkoumat jednotlivé eventy a prohlédávat pomocí filtrů veškerá sbíraná data.	V DASHBOARDU Sentinelu přímo v konzoli pro search (Sentinel) dat normalizuje a parsuje, ke zdrojům přidá taxonomii a provede dotazy na základě taxonomie, ale i dle parsovaných položek). Data jsou zpracovávána v paměti, což zrychluje procesování dat. Na základě drop down analýzy lze přímo vytvořit optimalizovaný dotaz a ten znova spustí, aby v paměti byly jen relevantní položky. Přístup je možný i přes API.	Pro základní analýzu nástroj poskytuje obrazovku "Discover", ve které uživatelé mohou filtrovat pomocí uživatelského interface, zkoumat histogramy jednotlivých atributů nebo přistupovat k předpřipraveným analytickým pohledům. Pro pokročilou drop down analýzu se využívá nástroj Kibana. Zde je možné vybrat druh vizualizace (Pie chart, Data table, Line chart atd.), dále pak způsob agregování dat a vlastní pole pro agregaci. Výslednou vizualizaci lze dále upravovat případně pokračovat dále v analýze.	Veškeré nástroje pro zobrazování (alerty, vyhledávání, reporty, dashboardy, active listy apod.) jsou interaktivní a umožňují jednoduchým klikáním dle úpravit parametry hledání.
Funkcionalita	Umožňuje vaše řešení zobrazit zdrojový log v RAW podobě?	Systém je založen na tom, že veškerá data jsou ukládána v RAW podobě a jsou vždy z této RAW podoby i zpracovávána. Podle typu dotazu se mohou automaticky zobrazovat upravená nebo odvozená data, případně lze vždy jednoduchým kliknutím RAW data zobrazit.			Řešení ukládá logy v přijaté podobě v automaticky vytvářené přehledné a datumy označené hierarchické struktuře. Čímž lze s těmito logy pracovat i bez potřeby SIEMu. SIEM jako takový podporuje výběr zobrazených logů buď v normalizované či RAW podobě. Pořádané logy lze pak vyexportovat do CSV či XML pro externí zpracování.	Lze stáhnout logy z daného collectoru členěné dle zdrojů do komprimovaných souborů po hodinách. Součástí řešení je ochrana proti modifikaci logu a validaci této modifikace. Lze použít akci, která najde jeden konkrétní raw záznam dle uloženého raw ID a zobrazí na konzoli Sentinelu. Systémové a některé speciální eventy získané z klientů raw data nemají (to co se posílá do Sentinelu, je již předparsováno při použití agentů).		Je možné zobrazit log v RAW podobě, kde jde pouze o zobrazení. Také je možné raw logy ukládat do samostatného pole. Zde je však nutné počítat s většími nároky na úložnou kapacitu, protože raw log se ukládá navíc.
Integrace	Podpora integrace log kolektoru nabízeného řešení s WEF/WEC: - zadavatel bude v jednotlivých lokalitách poskytovat logy z vlastního prostředí Windows pomocí WEF/WEC - je toto pro účastníka podporovaný způsob sběru logů - vyžaduje účastník od zadavatele nějaké specifické na nastavení WEF/WEC	Collection vrstva podporuje i přímé přijímání zpráv pomocí WEF. Zprávy z jednotlivých strojů lze přímo posílat do našeho kolektoru. Pro správnou funkci je nutné importovat validní a důvěryhodný certifikát (případně i kořenový certifikát od certifikační autority).	Jedná se o podporovaný sběr.	Nabízené řešení poskytuje komponentu WinCollect, která je schopna přijímat forwardované eventy z Windows systému a dále je propaguje do SIEM řešení. Pomocí filtrování je možné omezit počet eventů, které se do SIEM řešení dostanou. Výrobce pro zpracování logů prostřednictvím WEC/WEF poskytuje podrobný design a postup. Zde popisuje, jak provést nasazení i pro velice rozsáhlé prostředí. Zákazník i tak může kombinovat více typů sběru najejdnou bez omezení. Např. sběr logů ze serverů provést s využitím instalovaného WinCollect agenta do serverů, oproti tomu sběr logů z masivního množství Windows stanic provést prostřednictvím WEC/WEF serverů.	Nabízené řešení poskytuje komponentu WinCollect, která je schopna přijímat forwardované eventy z Windows systému a dále je propaguje do SIEM řešení. Pomocí filtrování je možné omezit počet eventů, které se do SIEM řešení dostanou. Výrobce pro zpracování logů prostřednictvím WEC/WEF poskytuje podrobný design a postup. Zde popisuje, jak provést nasazení i pro velice rozsáhlé prostředí. Zákazník i tak může kombinovat více typů sběru najejdnou bez omezení. Např. sběr logů ze serverů provést s využitím instalovaného WinCollect agenta do serverů, oproti tomu sběr logů z masivního množství Windows stanic provést prostřednictvím WEC/WEF serverů.	Nastavení je potřeba, aby se data v winlog sbírala a bylo zřejmé, které logy se mají v SIEM sbírat. Na win serverech musí být agent WMI pro jejich přeposílání. Sentinel se již sám připojí do agenta a konfigurace toho, co se má sbírat je v collectoru Sentinelu definována. (tj. WinRM musí být povoleno WEF, pak může forwardovat Windows Event Logs do Windows s Windows Event Collector (WEC) service. Na tomto kolektoru pak běží Sentinel agent pro forward logů).	WEC/WEF je podporován. https://docs.teskalabs.com/logman.io/collector/wec/ co lecting-by-window-event-collector-wecwef	Tato metoda sběru patří mezi nativně podporované. Nevýžaduje speciální konfiguraci nastavení
Integrace	Podporuje řešení účastníka integraci se systémy evidence assetů za účelem jako je např. MS AD, JIRA Insight, MSSQL, pro zajištění kompletního životního cyklu zdroje logů – vytvoření, provoz, zrušení: - identifikace nových zdrojů logů, dle výskytu nových assetů v evidenci - identifikace zrušených zdrojů logů, dle výmazu/přesunutí assetů z evidence - identifikace změny role napojeného zdroje logů	LogManagement lze integrovat se systémy typu CMDB (evidence assetů). Dokáže detekovat nové logsource nebo naopak nefunkční. Toto lze porovnávat s exportem ze CMDB a lze i automatizovat akce (vytvořit tickety s požadovanou změnou). Zároveň tyto informace mohou sloužit k detekci výpadku zařízení nebo detekci výpadku posílání očekávaných dat.	Řešení umožňuje pomocí API a custom modulu propojení se SW třetích stran a řízením SIEMu prostřednictvím SW třetí strany.	Ano, pomocí komponenty XXXXXX Asset import a pomocí implementační automatizace Universal REST API Protocol.	Řešení podporuje integraci assets do SIEM, ale obvykle integračním bodem pro různé systémy je jednotný Asset Management systém, který garantuje správnost záznamů a ty pak SIEM pro své potřeby využívá. SIEM jako takový si nedává za cíl suplovat Asset Management. Zákazník by si měl sám u sebe vysvětlit, co bude autoritativním zdrojem těchto záznamů a nejde o to, zdali k tom používá AD, Jira Insight či něco jiného. Pokud mu takováto komponenta/funkcionalita chybí, měl by ji vybudovat i pro podobné IS bez ohledu na nasazení SIEM. Účastník je mimo jiné i Attlassian Platinum partner a Jira Insight používá, a také ví, jaké Jira Insight má omezení.	Exportem csv a importem listu pro korelace, případně přes mapy dat. Lze realizovat akce automaticky, případně napojením na Sentinel API.	Ano, řešení je možné integrovat se všemi uvedenými technologiemi za účelem evidence assetů (v nabízeném řešení se tato oblast nazývá "lookups").	Identifikace nových a zrušených zdrojů dle DB assetů - ANO Lze automatizovat i samostatný change management při změnách

Integrace	Podporuje řešení vytváření ticketu v ticketovacím nástroji JIRA včetně zpětné integrace při zavření ticketu v ticketovacím nástroji?	Přes JIRA API je zajištěna obousměrná synchronizace	Řešení umožňuje pomocí API a custom modulů propojení se SW třetích stran. Konkrétní ticketovací systém by byl napojen na základě rozboru možnosti napojení těchto dvou systémů.	Ano, pomocí komponenty XXXXXX Ticketing v rámci XXXXXX Security Monitor.	Řešení obsahuje v sobě v základu jednoduché workflow k řízení stavů alarm. Řešení také umožňuje spuštění skriptu nebo vyvinutí vlastních aplikací pro integraci se systémy třetích stran. V případě, že zákazník používá vlastní Service Desk nástroj, např. Jira Service Desk, což se u zákazníka této velikosti očekává, pak životní cyklus určité události/alarmu se odehrává přímo v Service Desk nástroji. Pak zpětná integrace ze Service Desk nástroje do SIEM a do jeho jednoduchého workflow nedává smysl a interní jednoduché workflow se nepoužije. Účastník je mimo jiné Atlasian Platinum Partner.	Sentinel má svůj ticketovací nástroj, kde lze řídit životní cyklus ticketu. Je možné řešit akci přenos do Jiry, zavření lze řešit přes API Sentinelu.	Integrace je podporována.	Integrace s JIRA je standardně podporována oběma směry
Integrace	Podporuje řešení upozornění na nově vzniklý alert v SIEMu skrze notifikaci v MS TEAMS?	V rámci Response Action u definice UseCase lze přidat odpovídající akci k vytvoření Notifikace přes MS Teams.	Řešení umožňuje pomocí SmartResponse custom modulů propojení se SW třetích stran.	Ano, pomocí komponenty XXXXXX Ticketing v rámci XXXXXX Security Monitor.	Řešení umožňuje spuštění skriptu nebo vyvinutí vlastních aplikací pro integraci se systémy třetích stran. Opět nedává smysl, aby různé komunikační kanály byly řešeny při v SIEM a splovali funkce Service Desk nástroje, např. Jira Service Desk. Service Desk si pak sám řídí workflow a pokud v rámci připraveného workflow bude nastaveno předání požadavku řešiteli kanálem MS Teams, pip přes jiný messaging a mail systémy, tak to provede a bude o tom v Service Desk nástroji patřičný záznam, který bude průkazný i při auditu.	Je nutno dopsat akci (pokud MS teams má zveřejněné stabilní API).	Integrace je podporována.	Lze realizovat přes API, nutná integrace zadavatelem pro zpřístupnění rozhraní MS Teams, dle dokumentaci Microsoftu
Integrace	Podporuje řešení vyčítání kontextových informací z asset DB jako jsou např. MS AD, JIRA Insight, MSSQL atd..	Data se buď pravidelně importují do LogManagementu/SIEMu, do speciální struktury a následně se pomocí těchto dat obohacují zobrazované informace. Případně lze i zajistit Workflow v rámci UI, kdy si uživatel po kliku vyžte doplňující informace. Technicky funkční je i možnost online integraci přes API. Tuto variantu ale nedoporučujeme z výkonostních důvodů.	Řešení umožňuje propojení s AD a vyčítání informací o daném uživateli, tyto informace se pak zobrazí v analytickém prostředí. Jiné integrace jsou také možné pomocí API a dodatečných modulů.	Ano, pomocí komponenty XXXXXX ETL v rámci XXXXXX Security Monitor.	I zde je vhodné, aby na straně zákazníka existoval důvěryhodný autoritativní zdroj záznamů Asset Managementu, ze kterého může SIEM svá výstupy obohatit. SIEM si neklade za úkol řešit nedostatky nedostatečného rozšířného Asset Managementu na straně zákazníka.	Lze napsat Akci nebo Integraci, pokud bude zveřejněné API koncové aplikace.	Integrace je podporována.	Z databázi lze vyčítat jakékoliv informace použít je pro obohacení stávajících logů, nebo jako samostatné logy
Integrace	Podporuje řešení vyčítání kontextových informací k IP adresám a assetům z vulnerability nástrojů jako jsou např. Rapid7 Insight VM, Qualis, Nessus	Pomocí Addonu lze přidat integraci s požadovaným Vulnerability nástrojem. Obecně lze integrovat jakýkoliv nástroj který má dostupné informace přes aplikační rozhraní.	Je podporovaná integrace VA nástrojů. Výsledky z těchto nástrojů lze pak použít pro ovlivňování vyhodnocování use-casů.	Ano, pomocí integračních aplikací v rámci IBM QRadar SIEM od jednotlivých výrobců nebo pomocí rozšíření XXXXXX Context Info app v rámci XXXXXX Security monitor.	V současnosti je podporováno 23 skenerů předních výrobců pro oblast vulnerability assessment/management.	Dle popisu zdrojů je nutno dopsat feed.	Integrace je podporována.	Zpracování logů z VM nástrojů je standardně podporováno, zároveň lze využít data pro asset management
Integrace	Umožňuje vaše řešení např. pomocí REST API získávat informace o alertech vygenerovaných komponentou SIEM? Například použití pro export do MS PowerBI.	Všechny funkce dostupné pro uživatele jsou také dostupné přes API. Lze i pravidelně exportovat data do souboru, případně posílat exportovaná data emailem, a také lze data odesílat na požadované API.	Řešení umožňuje pomocí API a custom modulů propojení se SW třetích stran.	Ano, všechny data v rámci SIEM jsou dostupná pomocí dokumentovaných API rozhraní.		Je zde kompletní popis api	Řešení nabízí rozsáhlé REST API, včetně API k tzv. "Alert Managementu". Další integrační možnost je real-time stream přes Apache Kafka.	Komponenty disponují API, které má velmi široký rozsah funkcí, včetně práce s alerty
Integrace	Umožňuje vaše řešení spolupráci s nástrojem Jupyter? Pokud ano, popište?	Předpokládáme, že se jedná o Jupyter Notebook. Podporovaná verze je pomocí CLI a nebo pomocí Python scriptu. V případě CLI je toto popsáno přímo na stránkách Splunku v Blogu. Pomocí Splunk CLI se spustí požadovaný search a výsledek se generuje na standardní výstup. Z něj si ho vezme Jupyter Notebook.	Kooperace a integrace s platformou Jupyter Notebook pro ThreatHunting se popisuje zde: https://logrhythm.com/webcasts/upercharging-logrhythm-using-jupyter-notebook-to-enhance-threat-hunting/	Pro zodpovězení otázky potřebujeme více informací o systému Jupyter a zamýšlené integraci.	Informaci o existenci nástrojů Jupyter vidíme poprvé, na světě jsou milióny různých nástrojů a v tuto chvíli jsme nehodnotili, co je účelem takového neznámého/málo rozšířeného openource nástroje. Ani výrobce si nedává za snahu takového nástroje vyhodnotit a někde uveřejňovat takovouto kompatibilitu. Proto výrobce spolehně ne standardizované protokoly a služby, kterými lze integrace provádět. Ani zde v požadavku není popsáno, jaký přínos/účel má požadovaná integrace přinášet.	Ale asi není žádný problém dopsat.	Nástroj Jupyter Notebook je v řešení plně integrován a je součástí dodávky. Je samozřejmě možné integrovat se i z externím Jupyter Notebookem. Integrace je řešena pomocí komponenty "Export", kdy jeden z cílů exportu je Jupyter Notebook, resp. souborový systém, který je přístupný z Jupyter Notebook. Jupyter Notebook pak může přímo přistupovat k datům vyexportovaným z Log Managementu / SIEMu.	Nutno detailně definovat jakou vyžaduje zákazník integraci s nástrojem
Integrace	Podporuje vaše řešení export logů např. pomocí REST API? Aby bylo možné jejich další využití např. v nástroji JPCERTCC- LogonTracer	Všechny funkce dostupné pro uživatele jsou také dostupné přes API, tedy včetně exportu dat na základě dotazu.	Export logů lze realizovat pomocí přesměrování toku informací prostřednictvím https://docs.logrhythm.com/docs/enterprise/client-console-administrator-guide/log-distribution-services	Řešení podporuje export dat pomocí API na základě libovolného vyhledávacího dotazu.	Výsledek exportu je CSV nebo XML souborový formát.	Existuje několik metod pro export logů.	Toto řeší komponenta "Integrační služba", která je součástí navrhovaného řešení.	Komponenty disponují API, které má velmi široký rozsah funkcí, včetně práce s alerty

Integrace	Uvedte způsob, kterým bude řešení umožňovat sběr logů z prostředí Cloud / SaaS služeb, jako je Microsoft Azure (prostředí IaaS, provoz virtualizovaných prostředků Zadavatele, management prostředí MS Azure).	Sběr dat z externích systémů (včetně Cloud / SaaS / IaaS / PaaS) se provádí pomocí Splunk Heavy Forwarderu. Jedná se o dedikovaný server, na který se nainstaluje příslušný Addon, který se pak pravidelně dotazuje na příslušné API externího systému a importuje data k zaindexování.	Pomocí připravených beats https://docs.logrhythm.com/docs/OCbeats/azure-event-hubs-beat	Řešení podporuje sběr pomocí nativních cloudových protokolů (AWS, Azure, GCP a další) a možnost napojit libovolné REST API pomocí univerzálního REST API protokolu. Pro neznámé typy logů je možné připravit vlastní parser pomocí grafického rozhraní (DSM Editor).	Řešení poskytuje celou řadu aplikací, které rozšiřují nativní funkcionality. Jedním z nich je například aplikace Cloud Visibility, která využívá napojení na Cloudové služby a dostává z nich logy do SIEM řešení.	Dle topologie a rozsahu sbíraných aktiv a) Přeposílání logů přes zašifrovaný kanál na Sentinel collector. b) Instalace kolektoru přímo v prostředí Cloudu a propojení kolektoru přes VPN přímo na nativní log. c) Přenos souborových logů zašifrovaným kanálem a jejich rozbalení na collector. d) Instalace celého SIEM Sentinel v virtualizovaném cloud prostředí a forwarding pasovaných dat do hlavního Sentinelu.	Logy z Microsoft Azure se sbírají pomocí Event Hub. https://docs.teskalabs.com/logman.io/collector/azureeventhub	Pro toto prostředí jsou k dispozici nativní konektory, které budou provozovány v cloudovém prostředí
Integrace	Uvedte způsob, kterým bude řešení umožňovat sběr logů z prostředí Cloud / SaaS služeb, jako je Microsoft M365 (Azure AD, MS Teams, MS Sharepoint, MS Mail, MS MFA).	Sběr dat z externích systémů (včetně Cloud / SaaS / IaaS / PaaS) se provádí pomocí Splunk Heavy Forwarderu. Jedná se o dedikovaný server, na který se nainstaluje příslušný Addon, který se pak pravidelně dotazuje na příslušné API externího systému a importuje data k zaindexování.	Pomocí propojení přes API Office365 Management Activity, API Office365 Message Tracking	Řešení podporuje sběr pomocí nativních cloudových protokolů (AWS, Azure, GCP a další) a možnost napojit libovolné REST API pomocí univerzálního REST API protokolu. Pro neznámé typy logů je možné připravit vlastní parser pomocí grafického rozhraní (DSM Editor).	Prostřednictvím rozhraní API výrobce Microsoft, způsob sběru logů je daný, a to pro veškeré produkty v rámci rodiny Microsoft 365. Využívá se tenant ID. Výrobce IBM jasně definuje seznam platform ke sběru logů a použitých mechanismů sběru včetně protokolů apod. A to i pro případy pokud možností sběrů logů je více (např. REST API, Syslog, JDBC,...)	Pokud služba bude poskytovat data do SIEM řešení.	Logy z Microsoft 365 se sbírají dle následujícího návodu: https://docs.teskalabs.com/logman.io/collector/microsoft365 Ve zkratce se jedná o sběr pomocí auditního logu Microsoft 365 doplněného o Message Trace pro emailové služby.	Pro toto prostředí jsou k dispozici nativní konektory, které budou provozovány v cloudovém prostředí
Integrace	Uvedte způsob, kterým bude řešení umožňovat sběr logů z prostředí Cloud / SaaS služeb, jako je Atlassian JIRA.	Sběr dat z externích systémů (včetně Cloud / SaaS / IaaS / PaaS) se provádí pomocí Splunk Heavy Forwarderu. Jedná se o dedikovaný server, na který se nainstaluje příslušný Addon, který se pak pravidelně dotazuje na příslušné API externího systému a importuje data k zaindexování.	Výrobce má pro nejvíce používané aplikace připraveny beats pro integraci s cloud technologiemi: https://docs.logrhythm.com/docs/OCbeats	Řešení podporuje sběr pomocí nativních cloudových protokolů (AWS, Azure, GCP a další) a možnost napojit libovolné REST API pomocí univerzálního REST API protokolu. Pro neznámé typy logů je možné připravit vlastní parser pomocí grafického rozhraní (DSM Editor).	Pro zpracování logů z Jira zatím není vytvořen parser od výrobce IBM, protože logů je velké množství, ale v podstatě se používá univerzální způsob sběru logů prostřednictvím REST API. Jira jako aplikace je spletenec různých modulů a často i placených pluginů 3tích stran a jejich logování může být různé. Obvykle se loguje audit log a podobné logy, kde je zajímavý bezpečnostní kontext. Nutné napsat vlastní DSM (device support module / parser) pro parsování příchozích logů z Atlassian Jira. Účastník je certifikovaným Atlassian Platinum partnerem.	Nutno dopsat proprietární řešení. Nastavit v JIRA konfiguraci odeslání event do SIEM.	V Atlassian Jira se zapne "Audit Log". Log collector pak logy odebírá pomocí Atlassian Jira REST API v nastavených intervalech.	Pro toto prostředí je nutné vyvinout vlastní konektory, které budou provozovány v cloudovém prostředí
Výkonnost	Zadavatel provozuje v rámci své infrastruktury řádově vyšší počty zařízení, pro které může být v budoucnu identifikována potřeba napojení na centrální systém Log management & SIEM. Jaká je možnost rozšiřování licencí a kapacit řešení: - v prvních etapách projektu, bude dodavatelem napojeno jen cca 10% celkového množství potenciálních zdrojů - další zdroje logů si bude zadavatel napojovat sám, s podporou dodavatele, v následujících letech užívání nástroje - v jaké škále je možné licence navýšovat? - v jaké škále a jakým způsobem je možné navýšovat výpočetní výkon a kapacity?	Licence se kupuje podle denního objemu dat. Lze ji kdykoliv rozšířit dokoupením další licence, tedy licence se počítají. Počet a typ LogSource neovlivňuje licenci a tedy lze kdykoliv přidat další typy nebo další LogSource. Licence se dokupuje s krokem 1GB/den. Protože se jedná o SW, lze kdykoliv rozšiřovat horizontálně kteroukoliv vrstvu systému. Obecně je doporučováno, aby přidání server měl podobný výkon - počet a typ CPU, RAM. Přidávání serverů lze teoreticky po jednom, ale s ohledem na požadavek vysoké dostupnosti je většinou nutnost přidávat servery do obou lokalit.	Navržené distribuované prostředí umožňuje další rozšiřitelnost ve výkonu a v uložení zpracovávaných dat. Licence se navýšují o požadované EPS/MPS.	Navrhované řešení má více variant licencování. Nabízí buďto licencování pomocí EPS (Events per second) kde je možné licence dokupovat dle potřeby nebo licencování pomocí MVS (managed virtual server), kde se licenci systémů, které posílají data do SIEM řešení. Výhodou tohoto modelu je neomezená kapacita EPS. Rovněž řešení podporuje volitelné komponenty DataNode, kam lze ukládat velké množství méně zajímavých logů, např. aplikačních logů či debug logů z R&D.	Navrhované řešení má více variant licencování. Nabízí buďto licencování na základě využitých jednotek EPS (Events per second) kde je možné licence dokupovat dle potřeby nebo licencování pomocí MVS (managed virtual server), kde se licenci systémů, které posílají data do SIEM řešení. Výhodou druhého modelu je neomezená kapacita EPS. Rovněž existuje DataStore licence, který odemkne neomezené logování pro funkci Log Management. Taková zákazníci si prakticky ověří, že potřebují, aby do korelací vstupovaly jen vybrané bezpečnostní logy či logy z bezpečnostních systémů. Zbytek je pak logován a prohlédáván bez korelací a je omezen jen velikostí přiděleného datového úložiska. Rovněž řešení podporuje volitelné komponenty DataNode, kam lze ukládat velké množství méně zajímavých logů, např. aplikačních logů či debug logů z R&D.	Licenci lze nastavit na počet EPS a tu případně dokupit (velikost diskového prostoru, počet kolektorů a HW náročnost lze postupně rozšiřovat, collector engine lze odělit od centrálního serveru).	Tento způsob nasazování je typický. Licence jsou odvozeny od počtu EPS (měsíční průměr). Navyšují se po "baličcích" po 500 EPS. Řešení podporuje postupné navýšování kapacit a to jak vertikálně, navýšováním kapacit jednotlivých serverů tak i horizontálně přidáváním dalších serverů do clusteru. Zde je pro ilustraci specifikace jednoho uzlu clusteru, při horizontálním růstu se pak cluster zvětšuje o takové servery: https://docs.teskalabs.com/logman.io/maintenance/hw-extendable-specification	Licenci je možné rozšiřovat v přírůstcích po 100, 250, 500, 1000, 2500, 5000, 10000, 25000 EPS. Licence pro LM a SIEM je možné rozšiřovat nezávisle. Rozšiřování výpočetní kapacity se provádí přidáváním dalších výpočetních a DB nodů (viz. Popis architektury), které se dělají pouze na úrovni administrace řešení. Na straně sběru a konfigurace logů nejsou potřeba žádné kroky.

Reference	Účastník uvede alespoň 2 své referenční zakázky a jejich parametry za poslední 5 let, kterými může prokázat své zkušenosti s návrhem, implementací a správou řešení Log management a SIEM v prostředí o rozsahu odpovídajícím požadavkům Zadavatele. - Název organizace - Počet zdrojů logů - EPS nebo GB/d - finanční objem zakázky	YYYYYY - implementace SIEM - objem dat: cca 50GB/d - počet zdrojů dat stovky - finanční objem: 5mil Kč YYYYYY - implementace LogManagement a Observability - objem dat: cca 1TB/d - počet zdrojů: tisíce - finanční objem: 2mil Kč YYYYYY - implementace SIEM - objem dat: cca 50GB/d - počet zdrojů dat stovky - finanční objem: 2mil Kč	1. Název zakázky: Dodávka a implementace LogRhythm SIEM pro YYYYYY Název organizace: YYYYYY Počet: 2000 MPS Předmět zakázky: Dodávka hardware, software, kompletní migrace z předchozí verze LR SIEM řešení, včetně migrace všech usecase, monitoring bezpečnostních událostí. Finanční objem: 24 mil. Kč Rok: 2020 2. Název zakázky: Dodávka a implementace LogRhythm SIEM pro YYYYYY Název organizace: YYYYYY Počet: 2000 MPS Předmět zakázky: Dodávka hardware, software, implementace, servisní služby Finanční objem: 7,5 mil. Kč Rok: 2021	Účastník během posledních 5 let realizoval několik obdobných zakázek, tedy dodávku SIEM, implementaci a podporu. Mezi referenční klienty mimojiné patří YYYYYY, YYYYYY, YYYYYY, bankovní instituce či operátor ICT služeb. Detaily k zakázkám poskytneme v případě zájmu v rámci dalšího jednání. Obecně se jedná o zakázky nad 3 mil Kč plnění a nasazení nad 5000 EPS.	YYYYYY, 1600EPS, YYYYYY 600EPS YYYYYY 600EPS	YYYYYY: 25 Aktiv/ 400 node, 7600 EPS 35G per Day, cena více než 1mil Kč-YYYYYY: 25 Aktiv/ 130 node, 2390 EPS, cena více než 1mil Kč -YYYYYY: 20 Aktiv / 100 node, 2000 EPS, cena více než 1mil Kč	Název organizace - YYYYYY - Počet zdrojů logů - více než 2000 zdrojů - EPS nebo GB/d - 11 000 EPS - finanční objem zakázky - více než 50 mil. Kč Název organizace - YYYYYY - Počet zdrojů logů - více než 2000 - EPS nebo GB/d - 10 000 EPS - finanční objem zakázky -	YYYYYY (1000 zdrojů, 5000 EPS, Více než 15M CZK) YYYYYY (4000 zdrojů, 15000 EPS, Více než 50M CZK)
Kvalifikace	Účastník uvede složení svého realizačního týmu k prokázání způsobilosti realizovat zakázku na dodávku řešení Log management a SIEM v prostředí Zadavatele. Uvede jmenový seznam osob s uvedením rolí (jedná se zejména o role zodpovědné za celkové řešení, seniorní produktový specialista, seniorní analytik/specialista pro oblast KB, infrastrukturní specialista a pod.), navržených pro realizaci zakázky, u každého Účastníka pak uvede jeho osobní reference, tj. údaje o jeho prokazatelné účasti na podobných projektech včetně informací v jaké roli působil a jak dlouho. Dále pak uvede u každého odbornou/produktovou znalost doloženou dosaženými certifikacemi, případně další relevantní informace.	ANLT - XXXXXX XXXXXX (Splunk Enterprise Certified Administrator, Splunk Enterprise Security Certified Admin, Splunk Accredited Sales Engineer I) - XXXXXX XXXXXX (Splunk Enterprise Certified Accredited Sales Engineer I, Splunk Accredited Security Analyst I) - XXXXXX XXXXXX (Splunk Enterprise Certified Architect) SEC - XXXXXX XXXXXX (CSSLP, Cyber OPS, CSAE, CNSP, ISMS Lead auditor, GSOC, SPLUNK Certified Power User, ATT&ACK Threat Hunting and Detection Engineering, ATT&CK Purple Teaming Methodology) - XXXXXX XXXXXX (CCIE Sec)	Jméno: XXXXXX XXXXXX - Senior SIEM Specialist Certifikace: LogRhythm Platform Administrator LRPA LogRhythm Security Analyst LRSA LogRhythm Certified Support Engineer Prince2 Project Management Projekty: Implementace LogRhythm SIEM a řízení SOC týmu v YYYYYY - od roku 2015 Implementace LogRhythm SIEM pro YYYYYY - rok 2021 Jméno: XXXXXX XXXXXX - Senior Security Specialist a SIEM analytik Certifikace: LogRhythm Platform Administrator LRPA LogRhythm Security Analyst LRSA Scoping and Archtitecting a LogRhythm Solution Certified Ethical Hacker Projekty: Výpomoc v SOCu v YYYYYY - od roku 2018 Jméno: XXXXXX XXXXXX - Senior Project Manager Certifikace: TOGAF 9 Enterprise Architecture Prince2 Project Management ITIL, IT Security Management	Účastník uvede jmenový seznam do nabídky v rámci výběrového řízení. Účastník disponuje realizačním týmem v rozsahu: 4x SIEM senior konsultant, 4x technický specialista - všichni s technickou certifikací pro IBM Qradar SIEM a dlouhodobými zkušenostmi na SIEM projektech realizovaných účastníkem.	Pro vyhodnocení těchto požadavků zadavatel neposkytl dostatečné množství času.	XXXXXX XXXXXX, Certifikát kurzu Architekt Kybernetické Bezpečnosti, Sentinel Administrace, SLES Administrator- XXXXXX XXXXXX, Certifikát kurzu Architekt Kibernetické Bezpečnosti, Sentinel Administrace, SLES Administrator- XXXXXX XXXXXX- XXXXXX XXXXXX	Pro projekt navrhujeme použití těchto rolí: 1 osoba - Projektový manager: - Certifikace: PRINCE 2 Foundation - Zkušenosti: Alespoň 2 zakázky obdobného charakteru, tzn. řízení projektu nasazení Logmanagement a SIEM nástroje u zákazníka 3 osoby - Specialista L1 supportu: - Certifikace: min. základní certifikace správy SIEM - stejná technologie jež je předkládána - Zkušenosti: Alespoň 1 rok na pozici Specialista L1 supportu 2 osoby - Specialista L2 supportu: - Certifikace: min. základní certifikace správy SIEM - stejná technologie jež je předkládána - Zkušenosti: Alespoň 2 rok na pozici Specialista L2 supportu.	Tabulka realizačního týmu je součástí přílohy. Zároveň přikládáme jejich CV
Podpora	Účastník uvede úroveň technické podpory, které nabízí výrobce řešení Log management a SIEM a popíše, jakou úroveň podpory doporučí pro řešení v prostředí Zadavatele.	Výrobce Splunk nabízí dvě úrovně podpory. Standard a Premium. Podpora se liší v Response Time a garanci vyřízení - viz https://www.splunk.com/en_us/customer-success/support-programs.html?locale=en_us S ohledem na budované redundantní řešení a s ohledem na jiné existující projekty doporučujeme využít pouze standardní podporu, která je již obsažena v ceně licence. Další nadstandardní podporu dodáváme jako smluvní partner výrobce.		Účastník v rámci řešení XXXXXX Security Monitor poskytuje maintenance a využívá podporu IBM Subscription & Support, více v dokumentu nabídky.	Toto by mělo primárně vycházet z interních procesů zadavatele, z jeho řízení rizik a plánů kontinuity. Jelikož logování a omezení jeho funkcionality neovlivňuje business organizace, je obvykle vyžadována podpora během pracovních dnů a hodin.	Standardní podpora výrobce přes support portál s možností vytvářet tickety na produkt.	Podpora je dostupná v 8/5 (CET, Praha) nebo 24/7 režimu. Zde doporučujeme 24/7.	Výrobce nabízí pouze 1 úroveň podpory nabízených produktů, v kategorii Premium support

Licence	Účastník uvede názvy produktů, typy licencí (perpetuální/subscribe, resp. trvalé/předplatné), způsob licencování (dle EPS, GB/den atp.) - jednotek a jejich množství které použije pro výpočet indikace nákladů.	<p>Splunk Enterprise - LogManagement</p> <ul style="list-style-type: none">- Volume / day (GB / den)- Subskripce licence včetně standardní podpory <p>Splunk Enterprise Security- SIEM</p> <ul style="list-style-type: none">- Volume / day (GB / den)- Subskripce licence včetně standardní podpory <p>Cribl Stream a Cribl Edge - sběr logů, ETL pro logy</p> <ul style="list-style-type: none">- Volume / day (GB / den)- Subskripce licence včetně standardní podpory <p>Všechny produkty jsou licencované podle varianty na 500GB resp 1000GB za den</p>	<p>Název produktu: LogRhythm SIEM</p> <p>Moduly: Core Threat Detection Endpoint Threat Detection UEBA (User Entity and Behavior Analytics) - poskytuje hloubkovou analýzu chování jednotlivých uživatelů.</p> <p>GDPR compliance</p> <p>Rozšiřitelné moduly: SOAR - Jednoduše automatizuje opakující se úlohy, automatizuje pracovní postupy a urychluje tak kvalifikaci hrozeb a jejich následné vyšetřování a reakci na ně. Shromažďuje forenzní data z podezřelého koncového bodu během investigace</p> <p>CloudAI - aplikuje algoritmy strojového učení a samo-zdokonalující se umělou inteligenci. Jde o plně integrovaný add-on, určen především pro detekci bez-signaturových a skrytých hrozeb</p> <p>Licencování: Licencování dle MPS - Message per Second.</p> <p>Většina výrobců průměr EPS (MPS) pro své licenční potřeby počítá hodinově. LogRhythm vypočítává tento údaj jako denní průměr (tedy 24x24 hodiny).</p>	<p>Pro realizaci zakázky účastník nabízí licenci vlastního řešení XXXXXX Security Monitor v rámci programu IBM ESA, kde součástí licencí je software IBM QRadar SIEM a softwarové rozšíření XXXXXX Toolset pro pokrytí specifických potřeb.</p> <p>Všechny licence jsou perpetuální s maintenance na 5 let. Výčet licencí je uveden níže:</p> <ul style="list-style-type: none">- 1 x ISM Software- 22 x ISM Node- 3 x ISM HA option- 1 x ISM Datastore- 8 x ISM 2500 EPS upgrade (pro variantu 2 pak 16x)- 1 x ISM Toolset ETL- 1 x ISM Toolset Ticketing- 1 x ISM Context Info	<p>Pro využití dotační výzvy je vhodné využít perpetuální licence, kdy většina částky se vyčerpá již při implementaci, obnovy jsou pak mnohem menší ve velikosti cca 1/4 původní částky. Pokud zákazník zakoupí perpetuální licenci, bude licenční oprávnění vypsané na jeho jméno. K tomuto zákazník s IBM uzavírá dohodu Passport Advantage, kde se určuje vztah mezi výrobcem IBM a koncovým zákazníkem.</p>	<p>Micro Focus Sentinel, typ licence: perpetuální/subscribe, způsob licencování: dle EPS a počtu devices</p>	<p>TeskaLabs SIEM</p> <p>TeskaLabs LogMan.io PLUS</p> <p>Licencováno dle EPS (měsíční průměr).</p>	<p>Varianta 1:</p> <p>ArcSight Recon Standard Edition 10,000 EPS SW E-LTU</p> <p>ArcSight Enterprise Security Manager Standard Edition 10,000 EPS SW E-LTU</p> <p>Varianta 2:</p> <p>ArcSight Recon Standard Edition 25,000 EPS SW E-LTU</p> <p>ArcSight Enterprise Security Manager Standard Edition 25,000 EPS SW E-LTU</p>
Harmonogram	Účastník navrhne rámcový implementační harmonogram projektu dle definovaných fází a jejich výstupů (v případě, že rozdělení do fází, nebo jejich výstupů není dle účastníka optimální, navrhne vlastní rozdělení doplněné o vysvětlení)	viz SZ_harmonogram.png	<p>ETAPA 1 – čas realizace 1-3 měsíce</p> <p>V první etapě se dodá systém, nakonfiguruje se, připojí do adresářových struktur, definují se role a napojí se vzorové logy podporovaných datových zdrojů.</p> <p>ETAPA 2 – čas realizace 6-12 měsíců</p> <p>V této části realizace se provede zaškolení administrátorů na dané řešení a provede se integrace podporovaných datových zdrojů dle variant 1 a 2.</p> <p>ETAPA 3 – čas realizace 6-12 měsíců</p> <p>V této etapě se vytvoří a odladí jednotlivé scénáře (use-cases) a definují se jednotliví konzumenti těchto výstupů.</p> <p>ETAPA 4 – čas realizace dle množství a zadání</p> <p>V této části realizace se provede integrace specifických zdrojů dat, které nejsou nativně podporované výrobcem. Tato kapitola se odvíjí od počtu a složitosti těchto zdrojů dat.</p> <p>Celková doba zakázky by neměla překročit 24 měsíců.</p>	<p>Vzorový scope implementace je uveden sekci 5.1 nabídky, které lze rozdělit do 3 fází uvedených v poplávce. Samotný harmonogram bude záviset na počtu a druhu zdrojů logů a na požadavcích na korelační pravidla případně na další integrace.</p> <p>Minimální doba dodávky projektu je cca 6 měsíců</p>	<p>Pro vyhodnocení těchto požadavků zadavatel neposkytl dostatečné množství času.</p>	<p>Analýza zdrojů dat – Získání napojení zdrojů dat na síťové vrstvě (metodika doručení dat do SIEM systému síťová komunikační matice) – Napojení jednotlivých aktiv a analýza obsahu dat, které mají být přijímány – Nastavení filtrace – Analýza aktiv s pohledu auditu a nastavení auditu na datech – Nastavení agentů u zdrojů které neumíjí bez agentní zasilání dat.</p> <ul style="list-style-type: none">- Normalizace přijímaných zdrojů dat – Parsování přijímaných zdrojů dat – Nastavení taxonomie přijímaných dat- Dopsání kolektorů pro specifická data (která nejsou řešena v obvyklých standardních kolektorech, případně dopsání customizace standardních kolektorů – Nastavení rolí pro systém (oddělení obsahu, která má být zobrazována jednotlivým rolím) – Nastavení zdrojů informací jako IP lokace a klasifikace zdrojů (poté, než se zdroj	<p>Etapa C. 1 – cca 4 měsíce</p> <p>Vstupní analýza prostředí, identifikace zdrojů logových informací, návrh postupu realizace dle upřesněného harmonogramu.</p> <ul style="list-style-type: none">- dodávka technologií LM & SIEM- Instalace satelitních i centrálních komponent- Konfigurace LM&SIEM v prostředí dodavatele, napojení na LDAP/AD- Napojení vzorových zdrojů logů:- Ze všech satelitních lokalit- Vybrány jednotky reprezentativních formátů logů <p>Etapa č. 2 - cca 3 měsíce</p> <ul style="list-style-type: none">- školení pracovníků SŽ (doporučujeme přesunout do etapy č.3)- Napojení všech nezbytných zdrojů logů s cílem: (zdroje a jejich počty a způsob napojení, budou součástí úvodní analýzy)- Napojení standardních zdrojů logů- Jedná se zdroj	<p>Z aktuálně dostupných informací není možné připravit rámcový harmonogram, pouze jsme schopni poskytnout seznam nezbytných kroků pro úspěšnou implementaci:</p> <ul style="list-style-type: none">- Implementační analýza- Příprava prostředí- Konfigurace prostředí- Integrace zdrojových systémů- Tvorba use cases a obsahu pro LM a SIEM- Zaškolení- Dokumentace- Testování
Architektura	V souvislosti se schválenou strategií IS/ICT SŽ, a to konkrétně cílem zajištění dlouhodobého koncepčního a efektivního rozvoje IS/ICT prosíme o vyjádření k možnosti využití tzv. Platformy SŽ 2.0. Pro poptávaný systém Log Managementu a SIEMu očekáváme využití Platformy SŽ zejména jako infrastrukturní službu, tj. v režimu IaaS. Rozveďte prosím detailněji, které části/moduly řešení jsou schopné a vhodné pro nasazení na Platformu SŽ, které nikoliv a proč. Požadavky na platformu prosím vyplňte v Příloze č. 4: Požadavky dodavatele na Platformu SŽ.	<p>Protože všechny komponenty jsou dodávány jako Software a protože všechny komponenty podporují i kontejnery, analýzíme se maximálně využít existující platformy jako je IaaS nebo PaaS. Veškeré komponenty mohou běžet v rámci Platformy SŽ 2.0. Požadavky jsou vyplněné v příloze č.4</p>	<p>Navrhované řešení plně využije platformu.</p>	<p>Pro vyhodnocení těchto požadavků zadavatel neposkytl dostatečné množství času.</p>	<p>Řešení běží na Linux SLES, jak fyzickém tak virtuálním plně vytváje dle dokumentu: https://www.sp-ravazeleznic.cz/documents/57004227/143127438/1t_Platforma+S%C3%BD.pdf/499ba021-f982-4b58-a15a-56ba56a4cf8d Pro zálohování lze použít jak SW IBM Spectrum Protect, tak SW NAS Synology</p>	<p>Využití Platformy SŽ 2.0 je možné.</p> <p>Z infrastrukturních služeb se jedná o VM a datové uložiště.</p> <p>Dále pak PAM, IDM, Active Directory, Zabbix (pro provozní monitoring). Zálohování a obnova je aplikována na instalaci, nikoliv na data (kvůli jejich předpokládané velikosti). Dále bude využito "Komunikační infrastruktury".</p> <p>Pro variantu 1 je třeba 3 ks VMs, pro variant 2 pak 6ks.</p> <p>Disková kapacita (200TB) je odhadována při 18ti měsíční online retenci. Pokud by byla požadována např. menší online retence a zavedení off-line retence, tak se toto číslo adekvátně změní (změní).</p>	<p>Počítáme s využitím Platformy SŽ pro všechny komponenty řešení, o konketorových serverů po LM a SIEM. Všechny komponenty jsou připravené pro provoz ve virtuálním prostředí. Pokud by zákazník preferovat použití některých komponent na fyzickém HW, je nutné toto uvést.</p>	

Podpora	Poskytuje účastník servisní služby v požadovaném režimu, který je specifikován ustanovením kapitoly „12. SERVISNÍ MODEL“. Zadavatel požaduje plnění v parametrech servisního modelu „B1 Závažný“?	Ano, společnost XXXXXX provozuje Helpdesk systém, na kterém mohou zákazníci hlásit svoje potřeby. L1 pracovních podpory obhospodařují otevřené tickety a případně si žádají o L3 podporu od interních odborníků.	Výrobce zajišťuje podporu 24/7, viz: https://logrhythm.com/services/gl-obal-support-services/ . Lokální podpora je po upřesnění a konzultaci.	Součásti ceny		standardní SLA služba		
Podpora	Poskytuje účastník funkce Service Desku v požadovaném režimu, který je specifikován ustanovením kapitoly „10. HELPDESK“. Zadavatel požaduje plnění Help Desku v režimu „Režim 1“ a úrovni „L3“?	Ano, společnost XXXXXX provozuje Helpdesk systém, na kterém mohou zákazníci hlásit svoje potřeby. L1 pracovních podpory obhospodařují otevřené tickety a případně si žádají o L3 podporu od interních odborníků.	Výrobce zajišťuje podporu 24/7, viz: https://logrhythm.com/services/gl-obal-support-services/ . Lokální podpora je po upřesnění a konzultaci.	Součásti ceny		standardní SLA služba		

	Kategorie	Dotaz v rámci PTK	Výstup z PTK pro přípravu TS
PTK I	Centrální vs. decentralizovaný sběr logů	Uvedte klíčová kritéria pro rozhodnutí, která varianta (centralizovaný / decentralizovaný sběr logů) je vhodná v jakých situacích.	Bylo provedeno rozhodnutí, že se bude aktivita LM řešit v režimu centralizovaného sběru logů (všechny logy sbírány na jedno místo).
	Transport logů od zdrojů logů (Log Sources) do Log Managementu	Uvedte, zda a jak vaše řešení přímo podporuje zajištění kompletního přenosu logů od zdroje až kmístu pro vyhodnocování logů.	Zadavatel se rozhodl využít možnosti poptat řešení včetně transportní vrstvy pro přenos logů od zdroje k centrálním úložištím.
	Vztah řešení Log Management a SIEM (Security Information and Event Management)	Pokud zadavatel plánuje budoucí nasazení řešení SIEM, je vhodné spojit takovou aktivitu s realizací řešení Log managementu? Jaké jsou výhody doporučeného přístupu?	Zadavatel vyhodnotil jako vhodné provést sloučení aktivit Log management a SIEM. Přípravy veřejné zakázky bude probíhat sloučeně pro aktivitu Log management a SIEM.
	Použití Log Management řešení pro více kontextů, např. zvlášť pro IT (Information Technology) a OT (Operational Technology)	Uvedte klíčová kritéria pro rozhodnutí, v jakých situacích je vhodné oddělit Log Management pro IT/OT a jaké z toho mohou plynout důsledky pro architekturu řešení.	Zadavatel nepožaduje vybudování separátního kontextu řešení pro sběr logů v OT prostředí a vyspecifikoval vybranou část zdrojů logů ze svých technologických sítí k připojení do poptávaného řešení Log management a SIEM.

	Kategorie	Dotaz v rámci PTK	Výstup z PTK pro přípravu TS
PTK II	Architektura	Zadavatel umožňuje využití dvojice datových center, k umístění a provozu centrálních komponent řešení Log management a SIEM. Navrhněte vhodný způsob využití těchto DC, např.: - budeme využívat jen pro účely archivace - nebo bude realizovaný plnohodnotný cluster - jiný způsob využití	Dle získaných odpovědí na dotaz upravil zadavatel své požadavky na využití dvojice datových center pro režim vysoké dostupnosti (HA).
	Architektura	Jaké budou účely a parametry využití propoje mezi dvojicí DC v Praze: - jaké jsou v navrhované variantě požadované parametry propoje dvou DC - jak bude ve vybrané variantě vypadat využívání propoje dvou DC: - forwardování událostí z jedné lokality do druhé - replikace na úrovni DB - vícenodové zpracování a parita dat	Dle získaných odpovědí na dotaz upravil zadavatel své požadavky na využití dvojice datových center pro režim vysoké dostupnosti (HA).
	Funkcionalita	Může být log collector virtuální?	Vzhledem k získání kladných reakcí na podporu virtualizace, byl do technické specifikace doplněn požadavek instalaci komponent dodávaného řešení do virtualizační platformy SŽ (HCI).
	Funkcionalita	Po jakou dobu či množství dat log collector umožní ukládat logy při nedostupnosti centrálního řešení ?	Odpovědit účastníků umožnili aby byla zvolena varianta 0-5 dní, přičemž parametry pro každý satelitní kolektor budou specifikovány v předimplementační analýze.
	Integrace	Podpora integrace log kolektoru nabízeného řešení s WEF/WEC: - zadavatel bude v jednotlivých lokalitách poskytovat logy z vlastního prostředí Windows pomocí WEF/WEC - je toto pro uchazeče podporovaný způsob sběru logů - vyžaduje uchazeč od zadavatele nějaké specifické nastavení WEF/WEC	Specifikováno v technické části ZD jako požadavek na integraci řešení s WEF infrastrukturou provozovanou SŽ.
	Integrace	Podporuje řešení vytváření ticketu v ticketovacím nástroji JIRA včetně zpětné integrace při zavření ticketu v ticketovacím nástroji?	Podpora požadavku uvedeného v dotazu umožnila, že dotazovaná funkcionálníta bude zohledněna jako mandatorní požadavek v TS.
	Integrace	Podporuje řešení upozornění na nově vzniklý alert v SIEMu skrze notifikaci v MS TEAMS?	Podpora požadavku uvedeného v dotazu umožnila, že dotazovaná funkcionálníta bude zohledněna jako mandatorní požadavek v TS.
	Integrace	Umožňuje vaše řešení spolupráci s nástrojem Jupyter? Pokud ano, popište?	Podpora požadavku uvedeného v dotazu umožnila, že dotazovaná funkcionálníta bude zohledněna jako mandatorní požadavek v TS.

Příloha č. 19: Požadavky na služby Platformy SŽ pro Log Management a SIEM

Základní informace

- Tento soubor je přílohou zadávací dokumentace veřejné zakázky "Log management a SIEM".
- V tomto souboru účastník zadávacího řízení vyplní své požadavky na služby Platformy SŽ pro Log Management a SIEM.
- Pro účely projektu Log Management a SIEM jsou určeny a povoleny k výběru pouze Infrastrukturní služby platformy.
- Detailní popis služeb je uveden v Příloze č. 4 zadávací dokumentace Platforma SŽ 2.0: Vymezení služeb.
- Pro účely projektu Log Management a SIEM jsou parametry infrastrukturních služeb uvedených v detailním popisu upřesněny, nebo nahrazeny následovně:
 - Článek 5.1.1 Platformy 2.0 – pro projekt Log Management a SIEM je upřesněno, že budou dodávány v rámci virtualizačního prostředí virtuální jádra, přičemž minimální frekvence používaných fyzických CPU je 2GHz.
 - Článek 5.1.2 Platformy 2.0 – služby datového úložiště jsou pro účely projektu Log Management a SIEM nahrazeny popisem uvedeným v rámci Přílohy č. 1 ZD Technická specifikace, článek 2.4.5. a následujícími technickými parametry:
 - COLD Storage poskytuje úložiště s minimální rychlostí 500 IOPS (operací za sekundu).
 - HOT/WARM Storage poskytuje úložiště s minimální rychlostí 2.000 IOPS (operací za sekundu).
 - Úložiště pro zálohování – Backup zálohování je realizována zálohovacími servery s diskovým polem a páskovou knihovnou
- Požadované služby musí pokrýt všechny infrastrukturní požadavky nabízeného řešení tak, aby jej bylo možné nasadit a provozovat v parametrech definovaných Zadávací dokumentací zadávacího řízení.
- Účastník veřejné zakázky vyplní požadavky nabízeného řešení na Platformu SŽ do formuláře na listu "Požadavky".
- Tyto vyplněné požadavky slouží jako podklad pro výpočet dílčích bodů pro dílčí hodnotící kritérium "Požadavky na služby Platformy SŽ" - výpočet probíhá na listu "Požadavky" na základě jednotkových hodnot uvedených na listu "Jednotkové_body"
- Instrukce k vyplnění jsou obsaženy na příslušném listu.

Obsah tohoto souboru

List	Popis listu	Odkaz
Požadavky VYPLŇUJE ÚČASTNÍK	Obsahuje: <ul style="list-style-type: none">- Instrukce k vyplnění formuláře- Formulář pro vyplnění požadavků účastníka na Platformu SŽ- Výsledný počet dílčích bodů za kritérium "Požadavky na služby Platformy SŽ"	zde
Příklad Nevyplňuje účastník.	- Zpracovaný příklad vyplnění požadavků	zde
Jednotkové_Body Nevyplňuje účastník.	Přehled bodového hodnocení pro jednotlivé služby Platformy.	zde

V tomto XLSX souboru upravujte pouze buňky označené těmito barvami:

	Buňky k vyplnění
	Buňky k výběru z předdefinovaných možností (Dropdown)

Seznam služeb, které si účastník může nakonfigurovat je uveden v tabulce níže. Detailnější popis těchto služeb najdete v Příloze č. 4 zadávací dokumentace "Platforma SŽ 2.0".

Služba	Popis	IaaS/PaaS	Kategorie služeb
Win.VMware.x86_64	Služba virtualizace s OS Windows	IaaS	Infrastrukturní služba
RHEL.VMware.x86_64	Služba virtualizace s OS RHEL	IaaS	Infrastrukturní služba
SLES.VMware.x86_64	Služba virtualizace s OS SLES	IaaS	Infrastrukturní služba

Popis:

Na tomto listu účastník definuje požadavky nabízeného řešení na služby Platformy SŽ pro Log Management a SIEM. Výpočet dílčích bodů hodnotícího kritéria "Požadavky na služby Platformy SŽ" probíhá dle interní nákladové náročnosti požadovaných služeb Platformy SŽ. Počet celkových dílčích bodů se vypočte následovně: počet kusů * (zvolený počet Core * jednotkové body + zvolená velikost GB:RAM * jednotkové body + + zvolená velikost GB:Backup * jednotkové body). Jednotkové body jsou uvedeny na listu "Jednotkové Body".

Instrukce:

Jeden řádek tabulky odpovídá jedné požadované službě.

Do sloupce **Služba (B)** účastníků vybírá požadovanou službu z Platformy SŽ

Sloupec **Typ služby (C)** automaticky doplní o jakou kategorii Služeb se jedná.

Ve sloupcích **Core (E)**, **GB:RAM (F)**, **GB:COLD Storage (G)**, **GB:HOT/WARM Storage (H)** a **GB:Backup (I)** účastník volí požadovaný sizing služby. Ve sloupci **Počet kusů (D)** účastník zvolí celkový počet kusů dané konfigurace. Obecně přípustné hodnoty jsou 0 a celá

Sloupec **Core (E)** obsahuje počet virtuálních jader v rámci virtualizačního prostředí, přičemž minimální frekvence používaných fyzických CPU je 2 GHz.

Ve sloupci **GB:COLD Storage (G)** účastník specifikuje kapacitní požadavky na diskové úložiště pro dlouhodobé uložení dat typu COLD storage, dle schématu víceúrovňové architektury úložiště, který je provozován na discích typu HDD. Tento typ úložiště je k dispozici jen v lokalitách centrálního zpracování dat, nikoliv v lokalitách, kde budou umístěny jen kolektory dat (logů). Tento typ úložiště je provozován v georedundantním režimu a nebude dále jinak zálohován. COLD Storage poskytuje úložiště s minimální rychlostí **500 IOPS** (operací za sekundu).

Ve sloupci **GB:HOT/WARM Storage (H)** účastník specifikuje kapacitní požadavky na provozní diskové úložiště kategorie HOT a/nebo WARM, dle schématu víceúrovňové architektury úložiště. HOT/WARM Storage poskytuje úložiště s minimální rychlostí **2000 IOPS** (operací za sekundu).

Ve clauzuli **GR-Rackun (T)** účastník certifikuje kanaritiní požadavek na clauzuli zálohování která je realizována zálohováním serveru c

Počet bodů za konfigurovanou službu je možné vidět ve sloupci **P**, přičemž součet za všechny konfigurované služby je uveden v buňce **C14** (Dílicí body kritéria "Požadavky na služby Platformy SŽ").

Dílní body hodnotícího kritéria "Požadavky na služby Platformy SŽ" dle požadavků na služby Platformy SŽ	-
--	---

Pro každou vybranou službu je povinné nenulovou hodnotou vyplnit sloupce B, D, E, F, sloupec I může nabývat i nulových hodnot. Dále je nezbytné vyplnit alespoň jeden ze sloupců G a H a dále sloupec O.

Seznam vybraných služeb musí pokrýt infrastrukturní požadavky nabízeného řešení tak, aby jej bylo možné nasadit a provozovat v parametrech definovaných zadávací dokumentací zadávacího řízení, zejména včetně pokrytí produkčního i testovacího prostředí (prosím označte ve sloupci Q), pokrytí potřeb zálohování a potřeb všech komponent - centrálních i satelitních.

Pokud se Vám zobrazují hodnoty **červeně, překročili jste povolený limit stanovený v technické specifikaci (2.4.12)**

[illegible]

Popis:

Na tomto listu je ukázán možný spôsob vyplnenia Požiadaviek na Platformu SŽ.

Celkové bodové ohodnocení požadavků dodavatele:	2334373
--	----------------

[illegible]

Bodové ohodnocení nákladnosti služeb v Platformě SŽ

Popis:
Dílčí body za jednotku IT služeb SŽ.
Tabulka slouží jako vstup pro hodnocení požadavků účastníka ve VZ (kritérium "Požadavky na služby Platformy SŽ").

Služba	Typ služby	Iaas	Body Základ	Body Core	Body GB:RAM	Body GB:COLD	Body GB:HOT/WARM	Body GB:Backup (COLD)
Win.VMware.x86_64	Infrastrukturní služba		0,00	553,66	46,14	1,54	2,29	1,00
RHEL.VMware.x86_64	Infrastrukturní služba		0,00	200,68	16,72	1,54	2,29	1,00
SLES.VMware.x86_64	Infrastrukturní služba		0,00	173,85	14,49	1,54	2,29	1,00

Licence

Účastník vyplní ve sloupcích C a D za každý potřebný typ licence, údržby licence a subskripce licencí jejich název a počet.
Požadavky na licence jsou definovány technickými požadavky na poptávané řešení.

Druh licence		Název licence	počet
Licence Log management a SIEM	Perpetuální licence		
	Údržba perp. licencí		
	Subskripce licencí		
Ostatní licence (OS apod.)	Ostatní licence - subskripce		
	Ostatní licence - perpetuální		
	Údržba ostatních licencí		

Požadovaná funkcionalita systému	Splnění požadavku (Ano/Ne)	Způsob naplnění
Architektura škáluje na běžném spotřebním hardware bez omezení na úložný prostor (možnost přidání hardware dle potřeby): - Horizontální škálování (přidání hardware výpočetního uzlu dle potřeby, clusterování) - Vertikální škálování (povýšení HW prostředků jednoho uzlu)		
Automatická komprese indexovaných dat pro redukci nároků na úložný prostor		
Celé řešení je možné spravovat pomocí Grafického rozhraní.		
Celé řešení je možné spravovat pomocí konfiguračních souborů, nebo přes API volání (pro řešení automatizace)		
Centralizovaná správa a monitoring funkčnosti všech SIEM komponent		
Flexibilní nastavení uchování dat s možností odstupňování řízení toho, co se stane s postupně stárnoucími daty. Neaktuální data mohou být přesunuta na externí (levnější) datové úložiště k archivaci a (nebo) smazána.		
Flexibilní nastavení uchování dat: - Nezávislost na technologii uložení dat - Může uchovávat indexovaná data, jak dlouho bude potřeba – dny, měsíce, roky - Odstupňované řízení toho, co se stane s postupně stárnoucími daty. - Neaktuální data je možné řízeně provozovat na levnějším datovém úložišti a nebo smazána.		
Informace o času poslední dostupnosti každé z komponent SIEMu		
Instalovatelné na běžně dostupný hardware dle vlastního výběru, včetně virtualizace Vmware		
Instalovatelné na všechny hlavní operační systémy (Windows, Linux, HP/UX, AIX, FreeBSD, Solaris, ...)		
Jeden produkt integrující jak funkce pro Log management i SIEM (nejsou oddělená datová úložiště a uživatelská rozhraní pro Log management a SIEM)		
Jednotné uživatelské rozhraní pro všechny systémové funkcionality včetně vyhledávání, reportování, tvorbu pravidel, správu systému (transportní vrstva může mít samostatné uživatelské rozhraní)		
Možnost distribuované architektury – rozložení zátěže, redundance, rychlejší odezva management konzole a možností rozproštění dílčích systémových funkcionalit (rolí) mezi více prvků celého řešení s centrální správou		
Možnost instalace on-premis, v cloudu nebo kombinovaný hybridní přístup		
Možnost nasadit veškeré klíčové prvky v HA modu. V HA modu nemusí být části, které při výpadku krátkodobě (min 1 den) neovlivní jakkoliv funkcionalitu systému		
Možnost přístupu a vzdálené správy přes WebUI a CLI		
Možnost snadno přeposílat data do jakéhokoliv externího systému nebo logovacího nástroje: - V době indexování mohou být původní data přeposílána protokolem syslog přes TCP, UDP nebo jako prostý TCP stream - V době indexování může systém přeposlat vybrané, transformované a/nebo o kontext obohacené události jako soubor nebo syslogem přes TCP či UDP		
Možnost využití nestrukturovaných souborů a datového skladu bez pevného schématu (bez relační database s pevným schématem)		
Musí podporovat vývojové nástroje (SDK) psané nad API pro jazyky, např.: - Python - Java - JavaScript - PHP - Ruby - C#		
Podpora instalaci do virtuálního prostředí i na fyzický hardware (bez omezení na konkrétní virtualizační platformu)		
Poskytuje webové rozhraní pro koncové uživatele (nevyžaduje instalaci tlustého klienta)		
Pouze software - bez vazby na uzavřenou fyzickou appliance		
Produkt bude integrovat jak funkce Log managementu, tak SIEMu. Nejsou oddělená datová úložiště a uživatelská rozhraní pro Log management a SIEM		
Řešení ukládá audit akci provedených administrátory Log managementu a SIEMu. Systém provádí nativně audit veškerých změn v konfiguraci, bez ohledu na to, jakým způsobem byla změna provedena, včetně přímého zápisu do konfiguračních souborů. Auditní logy se musí ukládat na jedno společné místo a všechna auditní data musí být dostupná a prohlédvatelná přes UI. Podpora odesílání auditních logů na úložiště mimo dodávané řešení Log management a SIEM, např. protokolem SYSLOG.		
Schopnost replikace dat k udržování násobku identických kopií indexovaných dat k zajištění dostupnosti a věrnosti dat, odolnosti proti neočekávané události (katastrofě) a zlepšení výkonnosti vyhledávání.		
Schopnost udržovat si původní časové známky pro každou událost a poradit si s časovými známkami z různých časových zón		
Schopnost uložit různá data do různých indexů pro optimalizaci vyhledávání nebo pro oddělení dat (řízení přístupu dle rolí uživatelů, tzv. RBAC)		
Schopnost vytvářet indexy a datová úložiště sumarizující surová strojová data a následně spustit vyhledávání/reporty nad těmito agregacemi pro zrychlení výkonu		
Systém není prototypem vyvinutým pro účel této zakázky; veškerou funkcionalitu musí být dodavatel schopen na vyžádání zadavatele demonstrovat		
Systém umožňuje kompletní správu řešení pomocí automatizačních nástrojů (ansible, Puppet a dalších)		
Systém umožňuje rozšíření pomocí dalších placených i neplacených modulů		
Systém umožňuje snadné vytváření vlastních modulů např. pro možnost zpracování specifického formátu vstupních dat		
Škálovatelná architektura, která nasazená u zákazníků zpracovává více jak 10TB dat denně		
Umožňuje vyhledávat nad distribuovaným úložištěm (uložená data ve vzdálených lokalitách)		
Veškerá systémová nastavení jsou konfigurovatelná přes uživatelské rozhraní (WebUI), příkazovou řádku (CLI) nebo změnou souborů		
Veškerou konfiguraci je možné uložit a spravovat jako kód ve strukturované textové formě (například yaml,json,xml a dalších)		
Všechny reporty a dashboards je možné upravit v WebUI nebo přímou editací příslušných konfiguračních souborů		
Výrobce poskytuje veřejné úložiště dostupných nadstavbových aplikací (modulů)		
Infrastruktura pro přenos logů od zdroje k centrálním úložištím musí podporovat oba směry komunikací, tedy: - PUSH, kdy spojení navazuje prvek na vzdálené satelitní lokalitě - PULL, kdy spojení navazuje centrální komponenta řešení Log management a SIEM		
Využívá implementace technologie MapReduce pro rychlé a distribuované vyhledávání		
Využívá nestrukturované soubory a datový sklad bez pevného schématu (bez relační databáze s pevným schématem, což může být úzkým hrdlem nebo kritickým bodem selhání)		
Zasílání alertů při výpadku komponent		
Systém v rámci HA nasazení podporuje Active-Active režim nebo Cluster se všemi aktivními členy, je tím zaručen bezvýpadkový provoz.		
Zpracování dotazů musí být rozloženo přes všechny členy, kde jsou uložena data. Přidáním nového člena dojde k dalšímu rozložení zátěže a tím pádem ke zrychlení zpracování dotazů.		
Systém nepotřebuje provádět reindexaci již uložených dat, pokud dojde ke změně ve zpracovávání (parsing/normalizace) dat. změna se okamžitě projeví i v historických datech).		

Řešení je možné provozovat v běžně používaných kontejnerových platformách (Docker, Kubernetes, ...).		
Systém umožňuje definovat kde jsou v rámci operačního systému uložena data, konfigurace a interní logy.		
Licence není vázaná na instalovanou topologii - počet lokalit systému Log management a SIEM		
Licence není vázaná na počet uživatelů ani počet zařízení zasílajících logy		
Licence nesmí omezovat výkon, nebo propustnost dat systému v případě překročení licence		
Licenční model je založen na objemu dat zpracovaných za 24 hodin, nebo počtu událostí za sekundu průměrovaných za časové období delší než 1 hodina, což umožní pojmout případné chvilkové špičky v objemu přijímaných informací.		
Při překročení objemu zpracovaných dat za den, nebo EPS za období delší než 1 hodinu, nedojde k zastavení/zahazování nových příchozích dat		
Systém umožňuje zpracovávat nárazové špičky zpracovávaných dat bez omezení		
Agent pro Linux, min. CentOS, Debian		
Agent pro Windows (min. Server 2008 R2)		
Datové zdroje zahrnují jakoukoliv aplikaci, operační systém nebo systém ať už fyzický, virtuální nebo v cloudu, půjde-li o člověkem čitelná data)		
Nebude potřeba vytvářet datové schéma nebo připravit vyhledávací dotazy ještě před indexováním		
Řešení bude schopno pracovat s novými zdroji dat nebo změnami ve formátech logů u existujících datových zdrojů.		
Řešení může indexovat víceřádkové nebo komplexní logy událostí		
Schopnost importovat data pro indexaci z Hadoop platformy		
Schopnost indexovat a připravit pro vyhledávání všechna originální data bez jakékoliv modifikace (bez normalizace/redukce dat)		
Schopnost indexovat všechna původní nemodifikovaná data a jejich zpřístupnění při vyhledávání a generování reportů (bez předem definovaného schématu nebo normalizace/redukce dat). Žádná data se indexováním nikdy neztratí.		
Schopnost přijímat data přes širokou škálu mechanismů využívajících agentů i bez nich: - Dodavatelem podporovaný "univerzální agent" - agent musí mít schopnost šířovat komunikaci na centrální komponenty log management řešení, zadržovat data v cache, rozkládat zátěž na více indexátorů, posílat data přes TCP, explicitně potvrzovat přijetí - Syslog - Netflow (Netflow v5, Netflow v9, sFlow, IPFIX) - SNMP události - XML - CSV - JSON - Windows WMI - Čtení ze souborů uložených lokálně na indexátoru nebo přístupných vzdáleně jakýmkoliv běžně dostupnými protokoly (CIFS, SMB, NFS, apod.) - HTTP protokolem přímo z aplikací - Proprietární protokoly (např. Checkpoint OPSEC LEA, HPE Arcsight CEF, apod.) <i>(Vlastní vstupny/Skriptované vstupny, modulační vstupny, vlastní technologické moduly)</i>		
Schopnost připojit se přímo do tabulky SQL databáze a extrahovat obsah pro indexaci		
Schopnost získat a automaticky analyzovat jakýkoliv zdroj dat (textových, binárních) bez omezení na konkrétní verzi nástroje. V případě, že systém v konkrétní verzi nebude schopen získat nebo interpretovat požadovaná data automaticky, musí být natolik robustní a flexibilní, že zákazník nebo dodavatel jsou schopni doplnit funkčnosti vlastními silami – kombinací prostředků systému nebo s pomocí externích nástrojů.		
Schopnost zpracovávat 1 TB dat denně		
Systém je schopen nad logy provádět datové obohacení a normalizaci. Normalizací se rozumí sjednocení formátu logů stejného typu z různých zdrojů. Log je extrahován a zaveden do příslušného jednotného schématu. Za normalizaci se nepovažuje prostá extrakce datových polí z logů.		
Systém provádí sběr libovolných logů z OS Linux, přičemž umožňuje sbírat výstupy custom skriptů		
Systém sbírá libovolné logy z OS Windows, včetně informací z komponenty Windows perfmom, přičemž umožňuje sbírat výstupy custom skriptů minimálně v jazyce Windows Powershell		
Systém umožňuje definovat kde jsou jednotlivá data uložena, v případě lokalit je možné definovat v jaké lokalitě mají být uložena		
Systém umožňuje tagování (označování) jednotlivých logů a událostí dle libovolných kritérií		
Systém zajišťuje dostupnost provozních a bezpečnostních logů v nezměněném tvaru, tak jak byl poslán ze zdrojového zařízení		
Systém zpracovává data z neomezeného počtu zařízení (do systému je možné zasílat data z jakéhokoliv počtu typu zařízení s neomezeným počtem datových zdrojů)		
Univerzální index: - Sběr a zpracování a uložení jakékoliv textové informace bez ohledu na zdroj, objem, rychlost, proměnlivost, rozmanitost a strukturu dat v reálném čase - Indexování všech informací v původním nezměněném tvaru - Automatické doplnění časové značky ke každé události, pokud chybí		
Uživatel může nastavit klasifikaci a normalizaci vstupních dat		
Zdroje dat nebo oblasti dat, které mohou být indexovány a jsou relevantní pro technologická prostředí: - SCADA zařízení - Systémy průmyslové automatizace (ICS) - Výrobní systémy (CNC systémy, výrobní linky) - Data z fyzických visaček zaměstnanců (badge) - Radiofrekvenční identifikátory (RFID) - GPS data - Vlastní aplikace - PCAP soubory		

<p>Zdroje dat nebo oblasti dat, které mohou být indexovány:</p> <ul style="list-style-type: none"> - Firewally a VPN - IDS/IPS systémy - Autentizační systémy (vč. LDAP a Active Directory) - DLP systémy - Anti-malware nástroje - Automatizované nástroje pro analýzu malware - Webová bezpečnost a webová proxy - Emailová bezpečnost - Skenery zranitelností - Monitory integrity souborů - Web aplikační firewally - Logy operačního systému (koncové stanice a servery) - Email server - Web server - DHCP/DNS - Network Flows (NetFlow, sFlow, Jflow, IPFIX, atd.) - Síťová zařízení (směrovač, přepínač, balancer zátěže, atd.) - Databáze a sálkové počítače (IBM zSeries, atd.) - Zařízení pro ukládání velkých objemů dat (NAS, SAN, atd.) - Logy hypervisorů (VMWare, KVM, Citrix Xen, Hyper-V) a virtuálních serverů - Tiketovací systémy (Service desky) - Záznamy o hovorech (CDR) - Mobilní zařízení a MDM systémy - Nástroje pro správu serverů a koncových stanic (MS System Center, atd.) - Hostovaná prostředí virtuální systémů MS AZURE, AWS, Google, Cloudové aplikace - Sociální platformy (Twitter, Facebook, Foursquare, atd.) - ERP and CRM systémy - Aplikace 		
Systém musí být schopen zpracovávat, vyhodnocovat a zobrazovat metrická data, přičemž podporuje práci s časovými řadami.		
<p>Integrace s CMDB databází (Change Management Database) nebo databází aktiv s informacemi o aktivech včetně:</p> <ul style="list-style-type: none"> - Jméno zařízení, IP, MAC, lokalita, důvěrnost, vztah k normám, apod. - <u>Umožní mapovat IP na jméno zařízení a naopak.</u> 		
<p>Integrace s korporátními adresáři (AD, LDAP, atd.) pro extrakci informací o zaměstnancích včetně:</p> <ul style="list-style-type: none"> - Uživatelská jména, křestní jména, příjmení, telefon, nadřazený, oddělení, lokalita, privilegia, atribut o sledování, začátek a ukončení pracovního poměru a další atributy zaměstnanců - Dovolí možnost korelovat více uživatelský jmen zpět k jedinému zaměstnanci 		
Možnost snadné integrace s lidsky čitelnými zdroji informací o hrozbách, ať už jsou zdarma, komerční nebo od jakékoliv třetí strany		
Možnost využití externích zdrojů dat pro obohacení událostí přidáním dalšího kontextu (souvislosti), a/nebo vytvoření specifitějšího korelačního vyhledávacího dotazu		
Nabízí REST API, aby externím systémům, aplikacím a dashboardům zpřístupnil indexovaná data, vyhledávací příkazy a další funkce		
Nabízí zdarma více jak 2000 veřejně dostupných nastavbových aplikací (modulů) pro integraci s produkty třetích stran, vytvoření případů užití a celkové zkrácení doby nutné k získu očekávaného výsledku		
Web API pro napojení softwaru třetích stran (zpracování událostí, logů, alarmů, seznamů)		
Upozornění na nové vzniklý alert v SIEMu je vyžadováno integrovat jako notifikaci s platformou MS TEAMS. Skupina definovaných příjemců obdrží notifikaci v platformě MS TEAMS v případě výskytu detekované události.		
Systém musí umožnit integraci s nástrojem "Jupyter Notebook" pro lepší podporu datové analytiky s využitím programovacího jazyka Python.		
<p>Řešení musí být schopné obousměrné integrace s tiketovacím systémem zákazníka (ATLASSIAN - JIRA) z důvodu:</p> <ul style="list-style-type: none"> - automatického zakládání alertů jako bezpečnostní tikety (SIEM -> JIRA) - synchronizace stavu řešení tiketu OPEN / CLOSED zpět do nástroje SIEM (JIRA -> SIEM) 		
Možnost přidat nové zdroje bezpečnostních informací, ať už volně dostupných nebo komerčních či proprietárních		
Možnost využití externích zdrojů dat pro obohacení událostí přidáním dalšího kontextu (souvislosti), a/nebo vytvoření specifitějšího korelačního vyhledávacího dotazu		
Nová externí data (threat feed, obohacení dat) mohou být aplikována na již dříve indexovaná data pro usnadnění vyhledání nebo reportování, které jde zpět do historie v řádu dnů, měsíců či let.		
Při normalizaci lze provádět datový enrichment (Doplnit jméno počítače na základě jeho IP adresy, doplnit lokalitu dle GEO informace, provést dotaz do LDAP apod.)		
Systém vede evidenci aktiv a identit a jejich klasifikaci, která je využívána pro výpočet kritičnosti události a incidentů. Evidenci je možno plnit ručně nebo z externích zdrojů		
Case management a definice workflow musí být integrální součástí SIEM řešení		
Dotaz do uložených dat může být tvořen manuálně přímo v dotazovacím poli nebo s využitím „průvodce“ (wizzardu)		
Dotazy umožní uživateli získávat data na základě kdo, co, kdy a kde		
Flexibilní a uživatelsky intuitivní vyhledávací jazyk pro tvorbu vlastních dotazů, reportů a korelačních pravidel včetně možnosti vytváření vlastních „parserů“ dat umožňujících samostatně a jednoduše tvořit bez závislosti na placené asistenci nebo rozšířeních tvůrce technologie či technologického partnera) – s využitím regulárních výrazů, průvodců (wizzards) apod. S pomocí vyhledávacího jazyka lze kdykoliv vytvořit jakýkoliv korelační scénář.		
Jednotlivé dotazy lze do sebe „vnořovat“		
Jednotlivé příkazy vyhledávacího dotazu je možné řetězit podobně jako v unixových systémech, čímž je vytvořena jedna komplexní podmínka aplikovaná na data v dashboardu		
Ke každému vyhledávání je možné zobrazit detailní (debug) informace pro odladění chyb ve vyhledávání		
Možnost zadání ad-hoc dotazu do vyhledávacího pole pomocí vyhledávacího jazyka		
Možnost definice vlastních vyhledávacích příkazů, které můžou být využity v grafickém prostředí pro vyhledávání a práci s indexovanými daty		
Možnost definovat workflow včetně provedení automatické a semiautomatické akce: až po ověření a schválení analytikem (ten prověří, zda se nejedná o false positive)		
Možnost definovat workflow včetně provedení automatické a semiautomatické akce: ihned po detekci incidentu		
Možnost prohledávat celý text na jakékoliv pole v indexovaných datech na základě klíčových dat a časových úseků v rozsahu konkrétní nebo relativní časové okno na úrovni M/D/m/s		
<p>Možnost prohledávat celý text, jakékoliv pole v indexovaných datech na základě:</p> <ul style="list-style-type: none"> - Klíčových slov - Časové úseky - Konkrétní nebo relativní časová okna na úrovni měsíce, dne, minuty, vteřiny - Logické operátory („AND“, „OR“, „XOR“, „NOT“, atd.) - Regulární výrazy - Syntaxe zástupných (wildcard) meta znaků 		

Možnost spustit více souběžných dotazů		
Možnost uložení finálního dotazu jako dashboard, report, alert nebo novou událost		
Možnost volitelného „vzorkování“ – rychlejší prezentace výsledků zobrazením každého n-tého paketu		
Musí podporovat využití Machine Learning nástrojů pro identifikaci opakujících se vzorů v datech, detekci anomálií a prediktivní analýzu dat		
Musí umožňovat nad daty provádět statistické výpočty a analýzy (min, max, median ...)		
Podpora akce: Odeslání emailu		
Podpora akce: Spuštění skriptu		
Podpora akce: Založení tiketu v interním case tracking systému		
Podpora akce: Zápis do souboru		
Podpora vyhodnocování událostí z webového rozhraní		
Provádět statistické operace pro nalezení extrému (anomálie)		
Schopnost stanovit "normál" a pak aplikovat výše uvedené statistické operace pro nalezení extrému (anomálie), jež může být pokročilou hrozbou (APT), na kterou nelze aplikovat signaturu		
Statistická analýza včetně: - Počet výskytů, počet unikátních výskytů, součet - Nejběžnější hodnoty, nejméně běžné hodnoty polí - Minimum, maximum - Průměr, modus, medián, atd. - Standardní odchylka, rozptyl - Identifikace anomálních hodnot ve výsledcích, které mohou být nepravdivé, neobvyklé - Statistická korelace mezi atributy - Shlukování událostí podle jejich podobnosti k sobě samým jako jedna událost - Ořezávání extrémních numerických hodnot ve vybraných polích při statistické korelaci - První a poslední nalezená hodnota - Percentil - Predikované hodnoty (dotaz se dívá na historická data, aby matematicky předpověděl budoucí hodnoty) - Sloučení, rozdíl nebo průnik individuálních nebo vícero výsledků hledání - Hledání vztahů mezi páry atributů porovnáním hodnot prvního atributu vůči hodnotám druhého atributu		
Systém umožňuje notifikaci přes email, SMS, MS TEAMS, s možností definovat pravidla pro zaslání na různé adresy podle kritičnosti zdroje nebo celkového vyhodnoceného rizika události		
Systém umožňuje vyhledávání log záznamů, událostí a incidentů dle zadané kombinace tagů a dalších podmínek (dle časových kritérií, typu zdroje, IP adresy, uživatele)		
Ve vyhledávacím dotazu je možné se odkázat na jakékoliv pole nebo atribut z přijaté události a v podmínce očekávat konkrétní hodnotu (např. uživatel je z konkrétní skupiny v Active Directory, IP adresa je z konkrétní sítě (IP rozsah, výčet IP, CIDR formát, atd.), název aplikace odpovídá regulárnímu výrazu nebo řetězci apod.)		
Vyhledávací dotaz může být jednoduše uložen, sdílen nebo upraven v rámci systému		
Vyhledávání a vizualizace pokrývají základní oblasti pro dohled a analýzu – přístupy, koncová zařízení, síťová komunikace, zúčastněné entity (lidé a zařízení)		
Vyhledávání může být v reálném čase nebo naplánované		
Systém umožňuje definovat jakékoliv vlastní příkazy. Tyto příkazy je možné používat minimálně v rámci vyhledávání, korelací a reportů. Vlastní příkazy je možné za sebou řetězit a není omezeno, v jaké části vyhledávání je možné je použít.		
Automatická aktualizace parsovacích pravidel pro zpracování logů od výrobce zařízení		
Definice časového okna pro sledování korelace (okno aspoň 1 týden)		
Desítky korelačních vyhledávacích dotazů: - Existující dotazy mohou být snadno modifikovány a vytvořeny tak nové dotazy - Každý dotaz má automaticky přiřazenu konfigurovatelnou hodnotu závažnosti, vlastníka a stav		
Detailní pohled na každý incident, který zahrnuje: - Automaticky doplněný kontext o aktivech a identitách z externích zdrojů - Původní události, které představují incident - Historie postupu zpracování události (workflow) – kdo, co, kde, kdy, jak, čím, ... - Rozbalovací nabídka možností ke každému relevantnímu poli, která usnadňuje směřovat vyšetřování další cestou - Rozbalovací nabídka možností ke každé události, která usnadňuje směřovat vyšetřování další cestou - Možnost manuálně změnit závažnost incidentu, vlastníka, status a stejně tak přidat k incidentu poznámku		
Hlídní prahových hodnot (např. počítání přenesených bajtů)		
Je možno sledovat stav řešení incidentů a měnit jejich důležitost		
Jeden dotaz nebo report může zahrnout všechna indexovaná data		
K dispozici musí být funkce typu „Tail“ zobrazující aktuálně přichozí logy na základě podmínek definovaných analytikem		
K incidentu je možno přiřadit výsledky dalšího vyhledávání souvislosti		
Každé korelační pravidlo má automaticky přiřazenu konfigurovatelnou hodnotu závažnosti, vlastníka a stavu (dotazu lze nastavit uvedené defaultní hodnoty)		
Korelace logů mezi různými zdroji a typy zařízení		
Korelace na základě počtu výskytů nebo naopak na základě chybějícího logu		
Korelační pravidla musí umožňovat provázání a vizualizace s frameworkem MITRE ATT&CK		
Modul pro sledování shody s nařízením GDPR		
Monitoring v reálném čase, varování na známé i neznámé (tzv. APT) hrozby		
Možnost definic korelace v grafickém rozhraní a jejich následné vyhodnocení nad zpracovanými daty		
Možnost definovat vlastní parsovací pravidla pro zpracování nepodporovaných logů na základě regulárních výrazů.		
Možnost manuálně změnit závažnost incidentu, vlastníka, status a stejně tak přidat k incidentu poznámku		
Možnost řetězení korelací		
Musí umožnit provádět pokročilé analytické behaviorální analýzy v reálném čase		
Porovnávání hodnot ve vybraných attributech události		
Řešení musí korelovat informace o správě identit a přístupů s ostatními strojovými daty shromážděnými v infrastruktuře, aby porozumělo chování uživatelů a identifikoval neobvyklou aktivitu uživatelů.		
Řešení musí poskytovat techniky detekce hrozeb včetně pokročilé korelace, rozpoznávání vzorů, blacklistu a whitelistingu a statistické analýzy		
Řeší všechny hlavní případy užití SIEM nástroje včetně (nejen): - Log management - Dokumentace a audit průběhu šetření v čase (log book) - Forenzní přístup (dashboards, nástroje, workflow) - Tvorba vlastních bezpečnostních reportů, reportů na soulad s normami, vizualizace - Monitoring v reálném čase, varování na známé i neznámé (tzv. APT) hrozby - Schopnost provádět korelace přes více datových zdrojů a hledání specifických vzorů - Dlouhodobá retenace dat		
Schopnost provádět korelace přes více datových zdrojů a hledání specifických vzorů		
SIEM počítá baselines pro identifikaci nestandardního chování konkrétních zdrojů logů		
SIEM umožňuje zpracování dat ze skenerů zranitelností		
Sledování odchylek vůči baseline		

Systém automaticky počítá míru rizika (risk score) pro jednotlivá aktiva a identity dle jejich klasifikace a reálné zjištěných událostí a incidentů		
Systém obsahuje 100+ připravených korelačních pravidel		
Systém obsahuje workflow pro podporu řešení detekovaných událostí a incidentů. Incidents je možno přiřadit řešiteli.		
Systém počítá risk score dle zdroje a cíle události nebo incidentu a na základě toho je stanovena závažnost aktuálně detekované události		
Systém průběžně hodnotí rizika a poskytuje up-to-date informace o stavu rizik		
Systém umožňuje automatické stahování Threat feed z internetu/externího zdroje dat		
Systém umožňuje automatické vyhodnocování událostí na základě informací obsažených v Threat feed		
Systém umožňuje přidávat Risk score na jednotlivé assety (uživatel, it zařízení, uživatelsky definované,...), čímž může být ovlivněna závažnost detekovaných událostí.		
Uživatel si může definovat vlastní parsing, který neovlivňuje další uživatele ani zbytek systému		
Ke každému incidentu obsahuje časovou osu, kde je možno sledovat veškeré akce řešitelů		
<p>Dostupné vizualizace by měly zahrnovat:</p> <ul style="list-style-type: none"> - Čárový graf - Časový graf - Plošný graf - Sloupkový graf vertikální - Sloupkový graf horizontální - Jediná hodnota s trendem (růst, pokles) - Koláčový graf - Bodový graf - Bublínový graf - Cíferníkový (budíkový) ukazatel - Graf typu teploměr (zobrazení hodnoty ve vztahu k rozsahu) - Geolokační mapa - Graf zobrazující rozložení hodnot v geografických regionech - Kruhový graf - Výplňový graf - Tabulky (vč. doplňkových funkcí jako jsou automatické sumy, procentuálních vyjádření, číslování řádků, atd.) 		
Každý uživatel má možnost definovat vlastní reporty		
Komplexní, efektivní zobrazení více metrik pomocí unifikovaných zástupných symbolů (síťový prvek, grafy, budíky, hodnoty apod.) s libovolným rozvržením po celé obrazovce včetně mapování symbolů a jejich aktuálních hodnot do grafického podkladu (síťová topologie, mapa apod.) pro názornější interpretaci		
Možnost exportu dashboardů do PDF souborů a naplánování jejich odesílání dalším uživatelům emailem		
Možnost integrace s externími vizualizačními nástroji (D3, Tableau, apod.) pro další grafické formy výstupu		
Možnost vytváření šablon reportů		
Přehledná evidence a audit využití licencí s včasným varováním o přiblížení se a překročení limitu		
Reporting v SIEMu musí nabízet výstupy podle ISO 2700x (přičemž požadujeme minimálně ISO 27002)		
Reporty a dashboards obsahují možnosti jednoduchého filtrování pomocí formulářových polí a pomocí uživatelům zůžit záběr jen na data, která je zajímavá		
Reporty jsou poskytovány ve formě grafů a tabulek, přičemž tyto mohou být obsaženy v jedno reportu vícenásobně		
Řešení musí umožnit snadné vytváření široké palety vizualizací (ne jen pevně dané, předpřipravené reporty)		
Snadný tisk událostí, tabulek a vizualizací		
Systém obsahuje předdefinované a modifikovatelné reporty		
Systém provádí audit veškerých změn v konfiguraci		
Systém umožní tvorbu bezpečnostních reportů, reportů na shodu s normami a vizualizace		
U všech grafů lze snadno změnit nadpis, legendu, popisy os a další nastavení		
Uživatelské rozhraní typu „drag and drop“ umožňuje jak ne-technikům, tak technikům vytvořit komplikované reporty bez nutnosti manuálního zadávání vyhledávacích příkazů nebo porozumění formátu základních dat		
<p>Více jak 150 reportů a dashboardů organizovaných do logických skupin pokrývajících (nejen):</p> <ul style="list-style-type: none"> - Celkové bezpečnostní riziko - Incidenty - Nezpracované události - Bezpečnostní analýzy - Externí zdroje hrozeb - Anomálie, extrémy - Audit systému samotného SIEM systému - Přehled korelačních pravidel s kontextem „story“ a všech náležitostí k realizaci 		
Vizualizace musí být schopné aktualizovat se v reálném čase		
Vizualizace musí být schopné jasně zvýraznit extrémy/anomálie vyžadující další pozornost a šetření		
Všechny reporty a dashboards mohou být plně modifikovány		
Všechny reporty a dashboards podporují možnost „drill-down“, čímž se lze dostat z high-level reportu/dashboardu k detailnímu reportu/dashboardu či k přímo původním událostem v řádu sekund		
Všechny vizualizace podporují procházení prokládáním s cílem přejít z přehledu do původních událostí ve vteřinách		
Flexibilní kontrola přístupu na základě rolí (RBAC) pro řízení přístupu uživatelů a přístupů přes API. Umožňuje omezovat přístup ke specifickým datovým zdrojům, datovým typům, specifickým pohledům, reportům a dashboardům.		
Generování hashe v době indexování. Systém umožní pomocí vyhledávání zjistit, zda s daty nebylo manipulováno		
Integrace s Active Directory včetně autorizace a autentizace		
<p>K dispozici jsou tyto metody autentizace:</p> <ul style="list-style-type: none"> - Lokální autentizace - Common Access Card - Vícefaktorová autentizace – s více možnostmi zadání sekundárních autentizačních údajů - LDAP/Active Directory - Proxy SSO - SSO přes SAML - SSO přes reverse proxy - Univerzální API pro skriptovanou autentizaci pro externí systémy (RADIUS, PAM, atd.) 		
Monitoring své vlastní konfigurace a využití s cílem udržet si kompletní, auditní záznamy o tom, kdo přistupuje k systému, jaké dotazy spouští, na jaké reporty se dívá, jaké konfigurační změny provádí a další		
Šifrovaný provoz mezi agentem a Log management a SIEM řešením s podporou uživatelských SSL certifikátů		
Tok mezi instancemi je zabezpečen pomocí certifikátů		
Zabezpečený tok dat mezi instancemi distribuované architektury přes SSL/TLS.		
Enterprise podpora v režimu 24/7/365 (email, telefon, webový portál)		
Široká aktivní komunita uživatelů a vývojářů diskutující otázky v odborných fórech.		
Webový portál s bezplatné a volně přístupnou kompletní a detailní produktovou dokumentací		